TP-LINK®

全千兆防攻击安全型交换机

TL-SG2224P

用户手册

Rev1.0.3

1910040089

声 明

目 录

第1章　用户手册简介

感谢您购买我公司 TL-SG2224P 全千兆防攻击安全型交换机！

本手册旨在帮助您正确使用这款交换机。手册中包括对交换机性能特征的描述以及配置交换机的详细说明。请在操作交换机前，详细阅读本手册。

1.1　目标读者

本手册的目标读者为熟悉网络基础知识、了解网络术语的技术人员。

1.2　本书约定

本手册中使用的特殊图标说明如下：

图标	意义
注意：	该图标提醒您对设备的某些功能设置引起注意，如果设置错误可能导致数据丢失，设备损坏等不良后果。
说明：	该图标表示这部分内容是对相应设置、步骤的补充说明。

本手册中出现的常用键名称及其意义：

名称	意义
返回	返回上一个配置页面。
提交	提交当前的配置。
保存配置	保存最终的配置。
注意： 每一个设置更改后，如果只点击“提交”，交换机断电重启后会丢失当前未保存的配置信息；点击“保存设置”，交换机保存当前的配置信息。建议您在交换机断电前单击“保存设置”，以免丢失最新配置。	
帮助	获得相应页面中的帮助文档以了解相关知识。
关闭	关闭当前窗口或页面。
全选	使当前所有复选框处于选中状态。
清空	使当前所有复选框处于未选中状态。
删除	删掉当前选择的条目。
禁用	禁止使用某项功能。
刷新	更新当前配置页面。
查找	查找需要的条目。

1.3　本书章节安排

第一章：用户手册简介。帮助您快速掌握本书的结构、了解本书的约定，使您更有效地使用本手册。

第二章：产品概述。首先向您简单介绍本产品及其特性，再详细介绍本产品的硬件结构。

第三章：配置指南。指导您如何登录交换机 WEB 管理页面。

第四章：基本功能配置指南。介绍并指导您使用本产品的基本功能。

第五章：高级功能配置指南。详细介绍了本产品所具有的高级功能，帮助您更全面的使用本产品。

附录 A：TpSupplicant 软件使用说明。

附录 B：常见故障处理。

附录 C：出厂设置。

附录 D：术语表。

附录 E：技术参数规格。

第2章 产品概述

2.1 产品简介

TL-SG2224P 交换机是深圳市普联技术有限公司自主开发的全千兆防攻击安全型交换机。本产品针对目前局域网中出现的安全问题，提供了 802.1X 认证和 ARP 攻击防护（智能绑定）安全功能，并且提供了可视化的 WEB 操作界面。特别为网吧用户开辟了网络优化版块，并针对网吧和中小企业的常见业务应用提供了简单可靠的网络优化配置方案。本产品可广泛应用于中小企业、网吧、酒店、医院等细分行业，可为用户提供高性能、低成本的全千兆安全解决方案。

TL-SG2224P 全千兆防攻击安全型交换机提供 24 个 10/100/1000M 自适应双绞线端口，以及 2 个 SFP 模块扩展插槽。SFP 模块端口与最后两个千兆 RJ45 端口 Combo 共享，即：使用了 SFP 模块端口时，共享的千兆 RJ45 端口将不能使用。

2.2 产品特性

- 符合 IEEE 802.3、IEEE 802.3u、IEEE 802.3ab、IEEE 802.3z 标准；
- 提供 24 个 10/100/1000M 自适应 RJ45 端口；
- 提供 2 个共享的 1000M SFP 光口；
- 采用两级用户管理方式，增强交换机的管理安全性；
- 全双工流控符合 IEEE 802.3x 标准，半双工采用 Backpressure 标准；
- 端口支持 N-Way 自协商功能，自动调整传输方式和传输速度；
- 支持 8K MAC 地址；
- 支持 MAC 地址自动学习、自动老化及老化时间设置；
- 支持静态 MAC 地址、过滤 MAC 地址、动态 MAC 绑定等地址表管理功能；
- 支持基于端口的 VLAN、基于 IEEE 802.1Q 的 Tag VLAN 和 MTU VLAN；
- 支持端口安全控制、广播风暴控制等功能；
- 支持基于端口的入口/出口带宽控制；
- 支持端口汇聚功能；
- 支持端口镜像和流量统计功能；
- 支持基于端口、IEEE 802.1p 及 DSCP 的优先级配置模式；
- 支持 QoS 功能；
- 支持基于端口、基于 MAC 地址的 802.1X 认证；
- 支持 IP、MAC、端口三元绑定；
- 支持 ARP 攻击防护安全功能；
- 支持组播侦听功能；
- 支持 NTP 功能；
- 提供方便易用的 WEB 可视化管理；

- 提供多级用户、身份过滤等安全管理功能；
- 提供电缆检测（VCT）功能。

2.3 交换机的外观

2.3.1 前面板

TL-SG2224P 交换机前面板由 24 个 10/100/1000Mbps 端口、2 个 SFP 光口、RESET 键以及相关的指示灯组成，如下图所示：

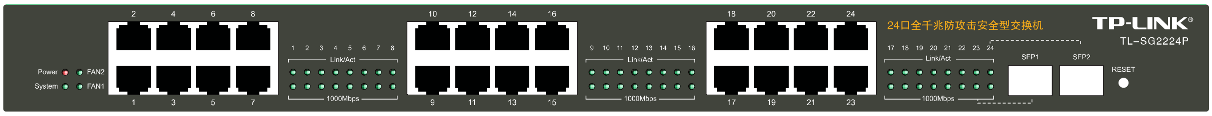


图 2-1 前面板

- **24 个 10/100/1000 自适应 RJ45 端口**

支持 10Mbps、100Mbps 或 1000Mbps 带宽的连接设备，均具有自协商能力。每个端口对应有一组指示灯，即 Link/Act 和 1000Mbps 指示灯。

- **2 个 SFP 模块接口**

2 个 SFP 模块卡扩展槽位于面板的最右边，同与其 Combo 共享的 RJ45 端口共用指示灯，其中 SFP1 与端口 23 共用，SFP2 与端口 24 共用。

- **RESET 键**

复位键。复位操作为：长按 RESET 键 5 秒，待所有指示灯一起闪烁 3 次后松开 RESET 键，交换机将自动恢复出厂设置并重启。恢复出厂设置后，默认管理地址是 192.168.0.1，默认用户名和密码是 supervisor/supervisor。

- 指示灯

指示灯	工作状态	工作说明
Power	常亮	交换机接上电源后，此指示灯为红色常亮
System	常亮	交换机接上电源后，此指示灯常亮，表示 CPU 中的软件运行正常
1000Mbps	常亮	当一个 10/100/1000Mbps 端口与 1000Mbps 设备连通时，相对应的指示灯为绿色常亮
	不亮	当一个 10/100/1000Mbps 端口与 10Mbps 或 100Mbps 设备连通时，相对应的指示灯不亮
Link/Act	常亮	当任何一个 10/100/1000Mbps 端口连接了一个网络设备，相应的指示灯为绿色常亮
	闪烁	当任何一个 10/100/1000Mbps 端口正常连接后，在接收和发送数据时，相应的指示灯为绿色闪烁
FAN	常亮	当风扇正常运行时，相应的 FAN1、FAN2 指示灯常亮

2.3.2 后面板

交换机后面板有一个电源插座。电源工作范围：100-240V~ 50/60Hz。

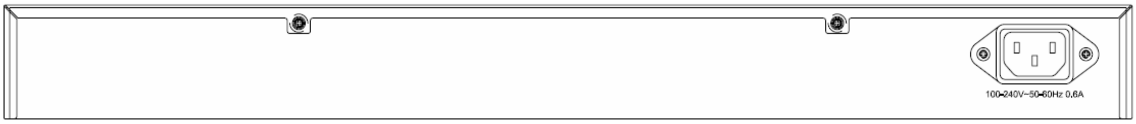


图 2-2 后面板

- **电源插座**

这是一个三相电源插座，电源线阴性插头与交换机电源插孔连接，阳性插头与交流电源连接。

第3章 配置指南

3.1 登录交换机

打开 IE 浏览器，在地址栏输入 *http://192.168.0.1* 登录交换机 WEB 管理界面，如图所示。



注意：

登录之前，请将计算机 IP 地址设置在交换机的 IP 网段。交换机 IP 地址出厂缺省为 192.168.0.1，需要设置计算机 IP 地址为 192.168.0.xxx，其中 xxx 为 2~254 中任意数字，子网掩码：255.255.255.0，默认网关：192.168.0.1。

打开交换机登录界面如 图 3-1 所示。



图 3-1 交换机登录界面

在此页面输入交换机管理帐号的用户名和密码，出厂缺省值为 supervisor/supervisor。

3.2 管理界面概述

经过上述步骤即可成功登录交换机管理界面首页，如 图 3-2 所示。在管理界面首页显示端口状态，其中“绿色”表示该物理端口已与设备连接。在端口状态下方可以查看交换机的系统信息。点击左上角的本公司的商标，您就可以很方便地访问本公司主页http://www.tp-link.com.cn。点击主页面左侧的导航栏即可进行相应功能的配置。



图 3-2 交换机管理界面

说明：

10 分钟之内没有对交换机管理界面进行操作，系统会自动退出管理界面，若要再次进行管理请重新登录。

3.3 功能概述

TL-SG2224P 交换机功能全面，除了系统管理、端口管理、地址表和系统工具等基本功能模块外，还具有 VLAN、ARP 攻击防护、组播和 802.1X 认证等高级功能。本手册将在以下章节中分别为您介绍。

第4章　基本功能模块

TL-SG2224P 交换机的基本功能包括**系统管理**、**端口管理**、**地址表管理**以及**系统工具**四个部分。

4.1　系统管理

点击**系统管理**，您可以看到：



4.1.1　运行状态

显示交换机当前的运行状态，包括端口状态以及系统信息。

4.1.1.1 端口状态

TL-SG2224P 交换机有 24 个 10/100/1000Mbps RJ45 端口以及 2 个 SFP 扩展模块槽，端口状态界面指示了它们的工作状态，其中以数字标识的端口是 RJ45 端口，标识为 SFP 的端口是光纤模块端口。端口图标呈现绿色表示该端口处于连接状态；呈现灰色表示该端口未连接；呈现黑斜杠表示该端口被禁用。其中模块端口指示了扩展模块槽的状态：呈现背景色表示没有插模块（如图 4-1）；灰色表示插有模块，但是没有连接(如图 4-2 的 SFP1)；呈现绿色表示插有 SFP 模块并处于连接状态（如图 4-3）。您也可以点击端口图标以获得该端口的更详细信息。



图　4-1 端口面板状态（无 SFP 模块）



图　4-2　端口面板状态（插有 SFP 模块但未连接）



图　4-3　端口面板状态（插有 SFP 模块并已连接）

点击某个端口时，将会弹出窗口显示此端口当前的状态信息。端口各种状态信息如图：

端　　口：	1
端口状态：	已连接
连接速率：	100Mbps
双工模式：	全双工
流量控制：	禁用

图 4-4 a 普通端口状态信息

端　口：	SFP1
端口状态：	--
连接速率：	--
双工模式：	--
流量控制：	--
模块类型：	未安装

图 4-4b 模块口状态信息（未安装）

端　口：	SFP1
端口状态：	已连接
连接速率：	1000Mbps
双工模式：	全双工
流量控制：	禁用
模块类型：	厂商： HI-OPTEL 型号： HSFP-24-3311S

图 4-4c 模块口状态信息（已安装）

说明：

1. 当端口没有建立物理连接或禁用时，“连接速率”、“双工模式”和“流量控制”三栏将显示“--”。
2. 端口状态的刷新时间默认为 30 秒。

4.1.1.2 系统信息

系统信息可以查看本交换机的硬件版本、软件版本、系统描述、系统标识及网络参数等基本信息。如下图：



图 4-5 系统信息

4.1.2 系统标识

系统标识用来设置交换机的标识信息，包括系统名称、系统位置、联系方法。

本页对系统标识进行配置，包括以下设置（如下图）：

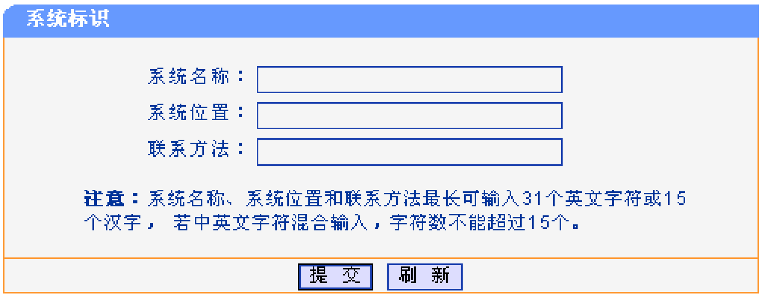


图 4-6 系统标识

4.1.3 网络参数

网络中的设备都有自己的 IP 地址。您可以手动设置交换机的 IP 地址、子网掩码和默认网关，也可以启用 DHCP Client 功能自动从网络上获取交换机的 IP 地址、子网掩码和默认网关。使用时应根据自己网络的实际情况对这些参数重新进行设置。

若网络中有一台 DHCP 服务器，并且要从这个 DHCP 服务器上自动获取交换机的 IP 参数，只需要启用 DHCP Client 功能，交换机将自动获取交换机的 IP 地址、子网掩码与默认网关，您可以在给交换机分配 IP 参数的 DHCP 服务器上了解到交换机的配置信息。

本页对网络参数进行配置，包括以下设置（如下图）：



图 4-7 网络参数

MAC 地址： 交换机的物理地址。MAC 地址在出厂时已被设定，用户不能修改。

DHCP Client： 选择 DHCP Client 功能是否启用。

IP 地址、子网掩码、默认网关： 这三项，可以结合 IP 寻址规则，给交换机设定我们需要的管理 IP 地址。比如现有局域网的 IP 地址规划为 172.16.1.0/24 这个网段的，为了方便对交换机的管理，我们可以在这里将交换机的管理 IP 设置为 172.16.1.X 并提交。

注意：

1. 当交换机获取到 DHCP 服务器分配的 IP 参数时，您可以在给交换机分配 IP 参数的 DHCP 服务器上了解到交换机的配置信息；当网络中没有 DHCP 服务器而启用了交换机的 DHCP Client 功能时，需要等待几分钟的时间，交换机会自动将 IP 地址参数中各项参数恢复为出厂设置。
2. IP 地址的变更可能导致当前网络连接的中断，请保持 IP 地址与局域网 IP 地址在同一网段。子网掩码的变更需要重启交换机才能生效。
3. DHCP Client 功能开启时，交换机将从网络中的 DHCP 服务器自动获取各项 IP 地址参数，所以此时“IP 地址”，“子网掩码”和“默认网关”均不能配置。
4. 交换机出厂时，DHCP Client 为“禁用”状态，默认的 IP 地址是：192.168.0.1。

4.1.4 用户安全

用户安全用来限制访问交换机 WEB 界面的用户属性，达到保护交换机设置的目的。登录交换机的 WEB 界面的用户属性分为“管理员”和“普通用户”。当以“管理员”身份登入 WEB 界面时，点击用户安全，您可以看到如下界面：



图 4-8 用户安全（管理员登录）

ID、用户名、类型： 显示“管理员”和“普通用户”的 ID 号、用户名和用户类型。

修改： 点击“修改”，可对于不同类型的用户修改登录密码等。修改

启用： 通过勾选来选择是否启用普通用户。默认为不勾选。

安全配置： 用于设定交换机的安全管理各项。安全配置

注意：

1. 该项目只有以“管理员”身份登录交换机才可以看到的。
2. 以下全部介绍如无特殊说明，均以“管理员”身份登录的 WEB 界面为准。

当以“普通用户”登录交换机 WEB 管理界面时，点击用户安全，您可以看到以下界面：



图 4-9 用户安全（普通用户登录）

4.1.4.1 修改

➢ 管理员用户修改

点击“管理员”后的“修改”，弹出如下界面：



图 4-10 管理员用户修改

本页面是针对管理员的属性进行修改。可以修改管理员的用户名以及登录密码。

➢ 普通用户修改

点击“普通用户”后的“修改”，弹出如下界面：

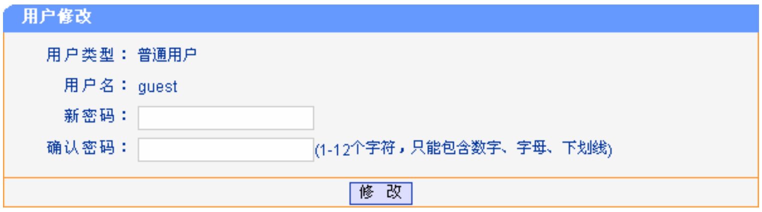


图 4-11 普通用户修改

本页面是针对普通用户的属性进行修改。可以修改普通用户的登录密码。

4.1.4.2 安全管理



图 4-12 安全管理

身份过滤： 用来选择身份过滤类型，分别为“IP 过滤”、“MAC 过滤”、“端口过滤”，默认选项为“禁用”。

➢ IP 地址、掩码：选择“IP 过滤”时才能填写，用来限定登录本交换机 WEB 管理界面的 IP 网段。只允许设置的 IP 地址和当前主机的 IP 地址可以访问交换机的 WEB 页面。其中掩码采用 255.255.255.255 类似的格式,将其与设置的 IP 地址进行与操作之后得到的 IP 地址段就作为可以访问交换机 WEB 页面的 IP 地址段。

- MAC 地址：选择“MAC 过滤”时才能填写，用来限定登录本交换机 WEB 管理界面的主机的 MAC 地址。只允许设置的 MAC 地址和当前主机的 MAC 地址可以访问交换机的 WEB 页面。
- 端口号：选择“端口过滤”时才能填写，用来限定登录本交换机 WEB 管理界面的交换机端口。只允许连接在所设定的端口上的主机访问交换机的 WEB 页面。

管理人数限制：　用来设定可同时登录交换机的管理员人数和普通用户人数，默认为“禁用”。

注意：

1. 当开启管理人数限制功能的时候，管理员及普通用户总人数不超过 17 人。
2. 即使没有启用限制人数功能，同时登录交换机 WEB 管理总人数也不能超过 17 人。

4.1.5 时间设置

系统时间是日程业务所使用的时间。您可以手动设置时间或者连接到一个 NTP(网络时间协议)服务器。如果您手动设置时间，您需要设置日期和 24 小时制时间。如果要设置 NTP 服务器，您只需设置时区。本页对时间设置进行配置，包括以下设置（如下图）：



图 4-13 时间设置

当前时间：　显示交换机当前的时间、日期、所处时区以及所选择的时间模式。

手动设置：　选择手动配置，直接在时间显示框内输入时间，点击提交即可。

NTP：　选择自动获得，如果手动配置了时间服务器的 IP 地址，交换机获取时间的时候会优先选择手动配置的时间服务器。如果没有设置时间服务器，交换机会选择网络上的时间服务器获取时间，但前提是交换机必须连接了 Internet。

获取管理 PC 时间：　选择此项，点击提交就可以将管理 PC 的时间设置为交换机的系统时间。

注意：

1. 这里的“时区”指的是选择“NTP”获得时间方式时所选择的时区；当选择“手动配置”和“获取管理 PC 时间”时无法对时区进行配置。
2. 交换机重启后时间设置会恢复为出厂设置，需重新设置交换机的时间。

说明：

获取的时间为 GMT 格林威治标准时间。

4.1.6 软件升级

本页提供交换机通过 WEB 方式升级系统文件功能。你可以在 http://www.tp-link.com.cn 网站上下载最新版本的系统文件。



图 4-14 软件升级

文件：	选择您要升级的系统文件。点击“浏览”，选择在主机中相应文件的位置。
软件版本：	显示当前系统的软件版本。
硬件版本：	显示当前系统的硬件版本。
升级：	点击此键，交换机将开始升级。

4.1.6.1 升级

点击**升级**，出现如下界面：

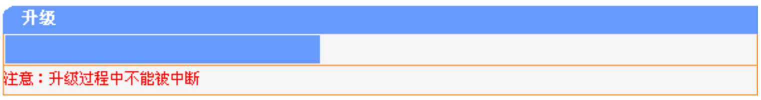


图 4-15 交换机升级

升级后交换机会自动重启，出现如下界面：

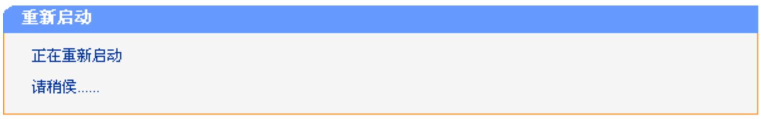


图 4-16 交换机自动重启

待交换机重启完成后，您可以重新登录交换机管理界面，此时交换机的软件版本为升级后的软件版本。

注意：

1. 升级过程中不能被中断。
2. 升级时请选择与当前硬件版本一致的软件。
3. 升级过程需持续一段时间，在此期间不能关闭交换机电源，否则可能导致交换机损坏而无法使用。
4. 当升级结束后，设备将会自动重新启动。

4.1.7 系统备份

本页提供交换机通过 WEB 方式备份和载入配置文件。如下图：

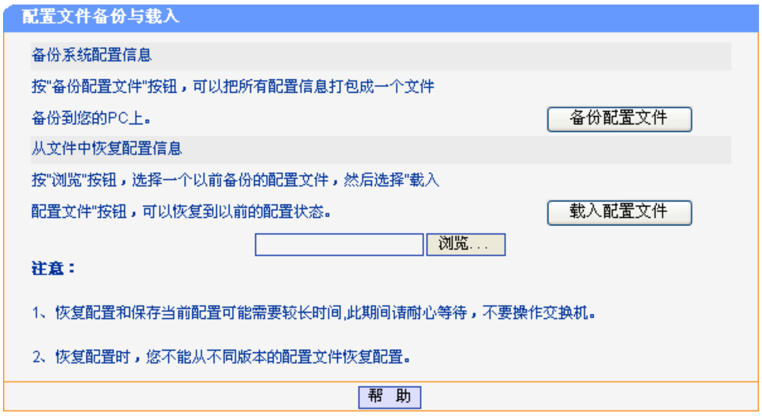


图 4-17 配置文件备份与载入

备份系统配置信息： 点击“备份配置文件”键，可以把交换机当前的配置信息以文件形式保存到您的交换机上。建议进行软件升级之前进行备份配置文件。

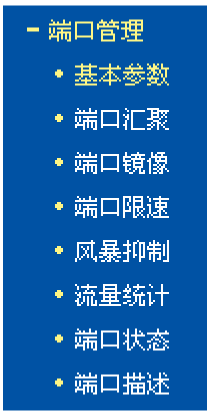
从文件中恢复配置信息： 点击“浏览”键，选择一个以前备份的配置文件，然后点击“载入配置文件”键，可以回复到备份的配置状态。

注意:

1. 恢复配置和保存当前配置可能需要较长时间,此期间请耐心等待，不要操作交换机。
2. 载入配置时，您的配置文件必须与当前的软件版本相匹配。
3. 导入配置文件后，交换机中原有的用户配置将会丢失。如果您载入的配置文件有误，可能会导致交换机无法被管理。
4. 载入配置文件的过程不能关闭交换机电源，否则将导致交换机损坏而无法使用。载入过程约 20 秒，当载入结束后，交换机将会自动重新启动。

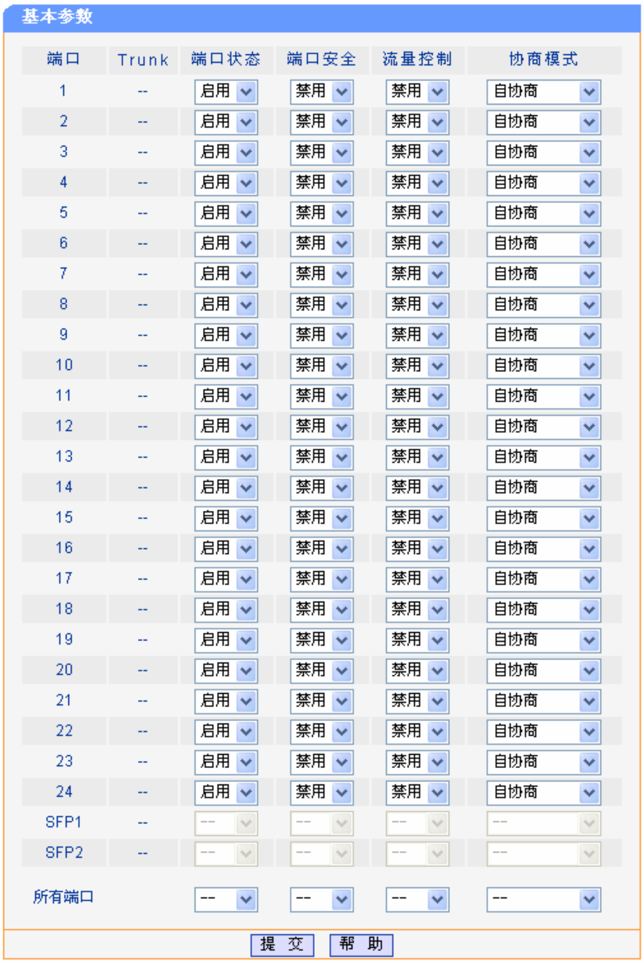
4.2 端口管理

点击**端口管理**，您可以看到：



4.2.1 基本参数

本页对交换机端口的基本参数进行配置，包括以下设置（如下图）：



基本参数

端口	Trunk	端口状态	端口安全	流量控制	协商模式
1	--	启用	禁用	禁用	自协商
2	--	启用	禁用	禁用	自协商
3	--	启用	禁用	禁用	自协商
4	--	启用	禁用	禁用	自协商
5	--	启用	禁用	禁用	自协商
6	--	启用	禁用	禁用	自协商
7	--	启用	禁用	禁用	自协商
8	--	启用	禁用	禁用	自协商
9	--	启用	禁用	禁用	自协商
10	--	启用	禁用	禁用	自协商
11	--	启用	禁用	禁用	自协商
12	--	启用	禁用	禁用	自协商
13	--	启用	禁用	禁用	自协商
14	--	启用	禁用	禁用	自协商
15	--	启用	禁用	禁用	自协商
16	--	启用	禁用	禁用	自协商
17	--	启用	禁用	禁用	自协商
18	--	启用	禁用	禁用	自协商
19	--	启用	禁用	禁用	自协商
20	--	启用	禁用	禁用	自协商
21	--	启用	禁用	禁用	自协商
22	--	启用	禁用	禁用	自协商
23	--	启用	禁用	禁用	自协商
24	--	启用	禁用	禁用	自协商
SFP1	--	--	--	--	--
SFP2	--	--	--	--	--
所有端口		--	--	--	--

提 交　帮 助

图 4-18 基本参数

Trunk： 查看端口是否为汇聚端口。

端口状态： 端口有“启用”和“禁用”两个状态。端口被禁用时交换机将丢弃来自这个端口的数据包。当交换机端口长时间不使用时，可以将该端口设为禁用，可有效减小交换机的功耗，待使用时再将该端口设为启用。

端口安全： 当某个端口启用端口安全后，该端口将不学习新的 MAC 地址，并且只转发来自已学习到的 MAC 地址的数据帧，其它的帧将被丢弃。当端口安全选择“禁用”时，该端口将自动学习新的 MAC 地址，转发收到的帧。

流量控制： 流控功能有“启用”和“禁用”两个状态。流量控制是为了同步接收方和发送方的速度而进行的控制。当接收方接收能力比发送方的发送能力小的时候，如果没有流量控制就会丢失数据。

协商模式： 交换机提供 N-Way 自协商功能。该功能使交换机的端口可根据另一端设备的连接速度和双工模式，自动调节速度和双工模式到双方都可以达到的最高水平，实现自动调整传输方式（全双工或半双工）和传输速度（10Mbps，100Mbps，1000Mbps）的功能，也可以手动设置交换机的传输方式和传输速度。

注 意：

1. 端口状态设置为禁用则不能通过该端口管理交换机，请将要进行管理的端口设置为启用状态。
2. 当某个端口的端口安全关闭时，该端口将开始自动学习新的 MAC 地址。

3. 当某个端口的端口安全启用时，不可以使用这个端口构成 Trunk。
4. 当某个端口已经设置了动态地址绑定后，不可以手动改变该端口的端口安全状态。
5. 在没有设置静态 MAC 地址的情况下，启用所有端口的端口安全，将导致无法管理交换机。
6. 虽然 SFP 模块支持热插拔，但由于交换机仅支持静态不同模式的配置，所以在 UTP、1000M SFP 和 100M SFP 间切换后，请手动更改相应共享端口的协商模式参数，或重新上电，以保证设置正确。
7. 当使用 SFP 模块端口时，如果改变 SFP 端口的的传输方式或传输速度会导致 SFP 端口不能正常通信，请保持默认设置。

说明：

1. 此页面包含了便于用户设定的快速更改功能。打开“所有端口”一行的某个下拉框，然后点击要设置的选项，所有可设定端口的对应项都会更改为此选项。点击“提交”后设置生效。
2. 从属于一个 Trunk 组的所有成员端口的相应参数设置应该保持一致。

4.2.2 端口汇聚

端口汇聚是将交换机的多个物理端口汇聚在一起形成一个逻辑端口，同一汇聚组内的多条链路可视为一条逻辑链路。端口汇聚可以实现将多条链路汇聚成一条逻辑链路以增加带宽的功能。同时，同一汇聚组的各个成员端口之间彼此动态备份，提高连接可靠性。

本页对端口汇聚进行配置，包括以下设置（如下图）：

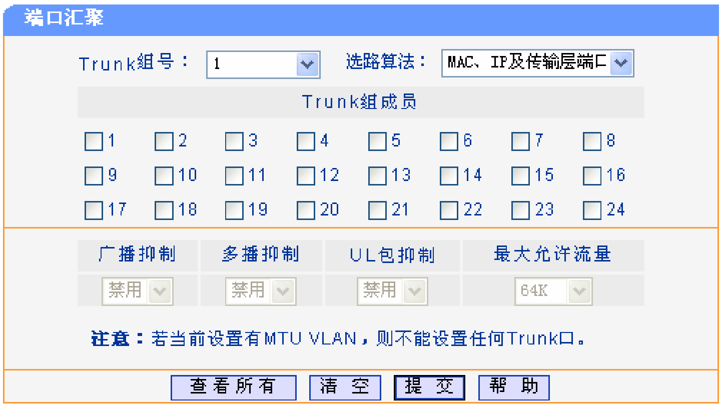


图 4-19 端口汇聚

Trunk 组号： 对应 Trunk 组的序号。“清空所有组”选项，表示不设置任何 Trunk。

选路算法： 根据选择的算法确定进行选路运算时交换机从数据包中需要提取的信息，并根据选路运算结果选择端口转发数据。

Trunk 组成员： 为 Trunk 配置成员端口，勾选中即为该 Trunk 成员。

广播/多播/UL 包抑制： 通过广播/多播/UL 包抑制功能，能够抑制网络中广播风暴的发生，保护网络安全。这里的广播风暴抑制设置是针对整个 Trunk 设置，各子项设置方法与端口的广播风暴抑制设置类似。

最大允许流量： 交换机对当前端口收到的三类包进行有选择的统计汇总（根据启用/禁用相应的抑制功能），并以最大允许流量指定的速率转发广播包，超出流量部分的广播帧将被丢弃。

注意:

1. Trunk 与 VLAN 之间的影响:

在设置 Trunk 的时候，Trunk 所有成员需要在同一个 VLAN 中，而且其缺省 VID 和 Un tag 帧处理规则需要一致。无论是创建、修改或删除一个 Trunk，其现有 VLAN 架构均不会改变。即，Trunk 不会改变既有 VLAN 的端口成员。

2. Trunk 与端口安全、端口监控、MTU VLAN 之间的影响:

设置成 Trunk 成员的端口不能再启用端口安全，并且不能设置为监控端口和被监控端口，反之一样。

若交换机当前启用了 MTU VLAN 模式，则不能设置任何 Trunk，相反，若设置了 Trunk 口，则不能启用 MTU VLAN 模式。

3. Trunk 带宽的计算:

当使用四个全双工 1000Mbps 端口构成 Trunk 时，由于每一个端口上行和下行各是 1000Mbps，所以每一个端口的带宽为 2000Mbps。它们使用 Trunk 技术聚合在一起形成的总带宽为 8000Mbps（2000Mbps X 4）。

4. Trunk 组的流量会根据选路算法均衡分配到各个成员端口中去。当 Trunk 组中的一个或几个端口连接断开的时候，这些端口的流量会转移到 Trunk 中其他链接正常的端口中去，即具备链路冗余备份功能。

说明:

1. 每个 Trunk 中的成员端口不能少于 2 个（页面上提交的成员可以为 0 个，此时表示该 Trunk 口没有生效或清除该 Trunk）。
2. 因为 Trunk 成员的行为都是一致的，所以这里的各个配置子项对于同一 Trunk 内各成员都是相同的。
3. 要删除一个已设置的 Trunk，将该 Trunk 的成员清空并提交即可。

4.2.3 端口镜像

端口镜像也叫端口监控。端口监控是一种数据包获取技术，通过配置交换机，可以实现将一个/几个端口（被监控端口）的数据包复制到一个特定的端口（监控端口），在监控端口接有一台安装了数据包分析软件的主机，对收集到的数据包进行分析，从而达到了网络监控和排除网络故障的目的。

本页对端口镜像进行配置，包括以下设置（如下图）:



图 4-20 端口镜像

监控模式： 有“输入监控”、“输出监控”、“输入输出监控”和“禁用”四种状态。这里的输入/输出是相对交换机而言的。

监控端口： 连接监控主机的端口。

被监控端口： 选择要被监控的端口，它可以是一个或几个端口。

注意：

1. Trunk 组的成员端口既不能作为监控端口，也不能作为被监控端口。
2. 一个端口不可以既作为监控端口又作为被监控端口。

4.2.4 端口限速

端口限速是通过带宽限制来控制端口（除模块口）的输入/输出数据传输速率。本页对端口限速进行配置，包括以下设置（如下图）：


端口限速

端口	Trunk	入口带宽限制	入口带宽	出口带宽限制	出口带宽
1	--	禁用	64K	禁用	64K
2	T1	禁用	64K	禁用	64K
3	T1	禁用	64K	禁用	64K
4	T1	禁用	64K	禁用	64K
5	--	禁用	64K	禁用	64K
6	--	禁用	64K	禁用	64K
7	--	禁用	64K	禁用	64K
8	--	禁用	64K	禁用	64K
9	--	禁用	64K	禁用	64K
10	--	禁用	64K	禁用	64K
11	--	禁用	64K	禁用	64K
12	T2	禁用	64K	禁用	64K
13	T2	禁用	64K	禁用	64K
14	T2	禁用	64K	禁用	64K
15	--	禁用	64K	禁用	64K
16	--	禁用	64K	禁用	64K
17	--	禁用	64K	禁用	64K
18	--	禁用	64K	禁用	64K
19	--	禁用	64K	禁用	64K
20	--	禁用	64K	禁用	64K
21	--	禁用	64K	禁用	64K
22	--	禁用	64K	禁用	64K
23	--	禁用	64K	禁用	64K
24	--	禁用	64K	禁用	64K
SFP1	--	--	--	--	--
SFP2	--	--	--	--	--
所有端口		--	--	--	--

注意： Trunk成员不能启用带宽限制。若端口已启用广播风暴抑制，则不能启用入口带宽限制。

提交 帮助

图 4-21 端口限速

入口/出口带宽限制： 启用或禁用入口带宽限制，限制相应端口的数据传输带宽。

入口/出口带宽： 若启用了带宽限制，这里选择的合适的带宽值，64K、512K、1M、2M、4M、16M、32M、64M、100M、256M，单位为 bps。

> **注意:**
>
> 1. Trunk 列提示的信息是根据当前交换机的 Trunk 设置显示端口从属于哪个 Trunk。Trunk 成员不能设置带宽控制。
> 2. 若端口已启用广播风暴抑制，则不能启用入口带宽限制。
> 3. 在一个或多个端口上启用出口带宽限制时，建议将各端口的流量控制禁用，以保证交换机的正常工作。

4.2.5 风暴抑制

广播风暴是指网络上的广播帧由于不断被转发导致数量急剧增加而影响正常的网络通讯，严重降低网络性能。广播风暴的判断标准为一个端口是否在短时间内连续收到许多个广播帧。广播风暴控制是允许交换机对网络上出现的广播帧进行过滤。当交换机发现广播帧超出一定的范围时，会自动丢弃广播帧，以防止广播风暴的发生。

交换机可以对三种常见的广播帧（广播包、组播包、未学习到地址的单播包）进行过滤。本页对广播风暴抑制进行配置，包括以下设置（如下图）：



图 4-22 风暴抑制

广播抑制: 对由普通广播引起的风暴进行的控制。

多播抑制: 对由组播引起的风暴进行的控制。

UL 包抑制： 交换机对未学习到地址的单播包进行广播，对由此引起的风暴进行控制。

最大允许流量： 交换机对当前端口收到的以上三类包进行有选择统计汇总（根据启用/禁用相应的抑制功能），并以最大允许流量指定的速率转发广播包，超出流量部分的广播帧将被丢弃。

注意：

1. 若端口已启用入口带宽限制，则不能启用广播风暴抑制。
2. 从属于 Trunk 组的成员端口属性将显示其所属 Trunk 的属性，且为灰色不可配置。

4.2.6 流量统计

流量统计针对每一个端口，统计它收发多少数据字节、多少个数据帧、多少个广播帧、多少个多播帧、多少个错误帧等等。



图 4-23 流量统计

总数据帧： 发送/接收的数据帧总数。

总字节数： 发送/接收的有效字节总数，（包含错误帧）。对于长度大于 10240 字节的数据帧，将按 10240 字节计算。

单播/组播/广播数据帧： 发送/接收的含单播/组播/广播 MAC 地址的数据帧数目（包含错误帧）。

碰撞数据帧： 发送数据帧时产生的碰撞（即冲突）数目。此项只有端口工作在半双工模式下才进行统计。

错误帧总字节数： 接收的长度无效（数据帧的有效长度为 64～10240 字节）的数据帧和校验和错误的帧总字节数。对于长度大于 10240 字节的数据帧，将按 10240 字节计算。

指定字节帧： 接收的长度为指定字节的数据帧数目（包含错误帧）。

小于 64 字节帧： 接收的长度小于 64 字节且包含合法校验字段的数据帧数目。

超长字节帧（合/非）： 分别统计接收的长度超过最大字节数(10240)并且包含合/非法校验字段的数据帧数目。

说明：

各统计项显示的最大值约为 1.8e+19，超过此数值将自动置零重新开始计算。您也可以通过点击页面上的“清零”键使全部统计项置零，重新开始计算。点击“刷新”键获取即时的统计数据。

4.2.7 端口状态

端口状态显示了每个端口的端口状态，连接速率，双工模式和流量控制。本页对端口状态进行查看，如下图：

端口状态

端口号	端口状态	连接速率(Mbps)	双工模式	流量控制
1	已连接	100	全双工	禁用
2	未连接	--	--	--
3	未连接	--	--	--
4	未连接	--	--	--
5	未连接	--	--	--
6	未连接	--	--	--
7	未连接	--	--	--
8	未连接	--	--	--
9	未连接	--	--	--
10	已连接	100	全双工	禁用
11	未连接	--	--	--
12	未连接	--	--	--
13	未连接	--	--	--
14	未连接	--	--	--
15	未连接	--	--	--
16	未连接	--	--	--
17	未连接	--	--	--
18	未连接	--	--	--
19	未连接	--	--	--
20	未连接	--	--	--
21	未连接	--	--	--
22	未连接	--	--	--
23	未连接	--	--	--
24	未连接	--	--	--
SFP1	--	--	--	--
SFP2	--	--	--	--

刷 新

图 4-24 端口状态

端口状态： 显示端口处于“已连接”、“未连接”还是“禁用”状态。

连接速度： 显示此端口当前的数据传输速度。

双工模式： 显示此端口当前的数据传输方式。

流量控制： 显示此端口当前的流控状态。

4.2.8 端口描述

端口描述是使用一个字符串描述一个端口，以便网络管理员分清楚各个端口的用途。

本页对端口描述进行配置，包括以下设置（如下图）：

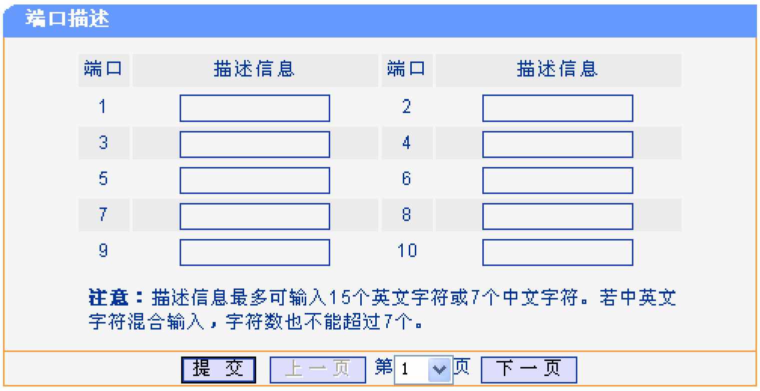


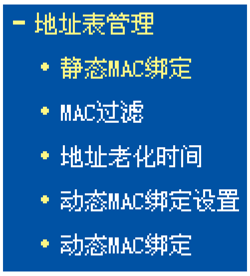
图 4-25 端口描述

端口： 对应交换机的物理端口。

描述信息： 此处填写描述文字。描述信息最多可输入 15 个英文字符或 7 个中文字符。若中英文字符混合输入，字符数也不能超过 7 个。

4.3 地址表管理

点击**地址表管理**，您可以看到：



4.3.1 静态MAC绑定

静态地址表记录了端口的静态地址。静态地址表中一个 MAC 地址对应一个端口，如果设置，则所有发给这个地址的数据只会转发给该端口。

静态地址是不会老化的 MAC 地址，它区别于一般的由端口学习得到的动态地址。静态地址一旦被加入，这个地址表项在被删除之前将一直有效，而不受最大老化时间的限制。这对于某些相对固定的连接来说，可以提高交换机的转发效率。

假设在静态地址表中设置了端口 1 对应的 MAC 地址为 00-0A-EB-00-00-01，那么，发给这个 MAC 地址的所有数据帧（目的地址是 00-0A-EB-00-00-01 的数据帧）只传递给这个端口。这对于某些相对固定的连接来说，由于减少了地址学习步骤，可以提高交换机的效率。同时也限制这个地址只能通过端口 1 连接到交换机上，达到易于管理的目的。

静态地址的设置需要正确输入 MAC 地址和这个 MAC 地址对应的端口。本页对静态 MAC 地址进行配置，包括以下设置（如下图）：



图 4-26 静态 MAC 地址表

查找： 在地址栏中输入要查找的静态地址并单击“查找”键。查找

添加： 在页面地址栏中输入要添加的静态地址，在“端口”下拉选择框中选择该地址对应的端口（默认为 1 端口），确认后单击“添加”键。只要满足以下条件添加操作都可以成功执行：

- 此 MAC 地址没有存在于静态地址表中，且该 MAC 地址为“启用”状态。
- 此 MAC 地址没有存在于过滤地址表中。
- 此 MAC 地址未被端口动态绑定。
- 静态地址表没有到达容量上限。
- 此 MAC 地址不是交换机的 MAC 地址。

当前状态： 显示该地址当前是否生效。

状态更改： 单击“启用”/“禁用”或“删除”键，相应的操作将被执行，并且地址的状态会立即刷新。

由于静态地址可能会配置得较多，本页面采用分页显示的方法，每页显示 10 条地址。您可以单击“上一页”，“下一页”或“首页”进行翻页。

注意：

1. 如果地址的端口指定错误，或使用过程中端口（或设备）被人为改变，必须重新设置该静态地址表项，否则交换机将无法正确转发数据。
2. 静态地址一旦被设置，如果把有此地址的网络设备连接到交换机的其它端口，交换机将不能动态识别。因此必须保证静态地址表中的表项都是正确有效的。
3. 凡是加入到静态地址表的地址，不能同时加入到过滤地址表，也不能被端口动态绑定。
4. 若 802.1X 模块开启，此功能禁用。

4.3.1.1 地址查找

点击“查找”后，如果找到了该地址，将显示以下页面：



图 4-27 静态地址表（查找找到）

您可以继续输入所要查找的 MAC 地址，并点击“查找”来进行再一轮的查找。

如果没有找到该地址，将显示以下页面，单击“返回”键返回：



图 4-28 静态地址表（查找未找到）

4.3.2 MAC地址过滤

MAC 地址过滤是通过配置过滤地址，允许交换机对不期望转发的数据帧进行过滤。在 MAC 过滤中添加受限的 MAC 地址后，交换机将自动过滤掉目的地址为这个地址的帧，以达到安全的目的。过滤地址表中的地址对所有的交换机端口都生效。

本页对 MAC 地址过滤进行配置，包括以下设置（如下图）。由于过滤地址对所有端口均有效，所以本页面没有任何针对端口的选项和显示信息，其余的操作与“静态 MAC 绑定”页类似，此处不再赘述。



图 4-29 过滤地址表

地址： 需要被交换机过滤的数据帧的 MAC 地址。

当前状态： 显示该地址当前是否生效。

状态更改： 单击“启用”/“禁用”或“删除”键，相应的操作将被执行，并且地址的状态会立即刷新。

注意：

1. 已加入到过滤地址表中的地址不能被加入到静态地址表中，也不能被端口动态绑定。
2. 若 802.1X 模块开启，此功能禁用。

4.3.3 地址老化时间

交换机内部总是维护了一张动态 MAC 地址表。动态 MAC 地址表有两项内容：MAC 地址及其对应的端口号。动态地址表是动态更新的，表里的每一个记录都是有寿命限制的，其寿命的长短受最大老化时间控制。如果该记录在寿命限定内没有被重新学习，那么它将会被删除，这个过程叫做“老化”。这个时间称为“最大老化时间”，单位为秒。

本页对 MAC 地址老化时间进行配置。包括以下设置（如下图）：

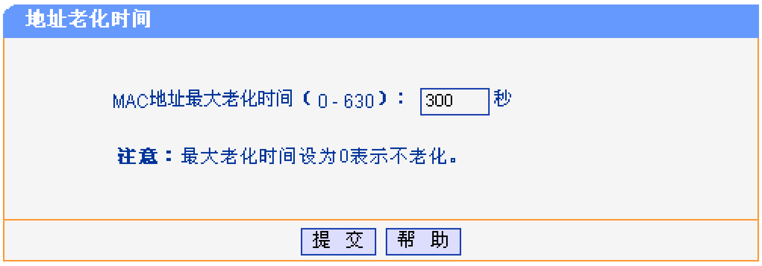


图 4-30 动态地址老化时间

动态地址老化时间（0~630）： 设定动态地址的老化时间，单位是秒。若该项设置为 0 表示地址不会被老化。

说明：

1. 最大老化时间的数值范围从 0~630 秒。老化时间过长会导致交换机内的动态 MAC 地址表中地址超期，从而导致交换机进行不正确的过滤/转发。老化时间过短，又会造成地址表刷新过快，大量接收到的数据包的目的地址在动态 MAC 地址表中找不到，致使交换机只能将这些数据包广播给所有端口，这将降低交换机的性能。
2. 静态地址表、过滤地址表以及动态绑定地址表中的地址不受最大老化时间的影响。

4.3.4 动态MAC绑定设置

动态地址绑定是指交换机的端口在动态地址绑定状态下，可以动态学习 MAC 地址，但是可以学习地址的数目是受到限制的。当端口学习到一个 MAC 地址后，立即被绑定，接着学习下一个地址。被绑定的地址不受老化时间的限制，会一直生效。端口学习到一定数目的地址后，就不再学习和绑定了。被端口绑定的 MAC 地址条目在该端口地址绑定功能被禁用或交换机重启后才会被删除。

这个功能的好处是，交换机启用该功能后，能自动绑定端口连接的计算机的地址。绑定的地址数达到允许的最大值后，就停止学习了。这样既能满足计算机上网的要求，也能提高交换机的效率，同时还能控制该端口上网的用户数。

设置端口地址绑定后最好重新启用交换机，让交换机重新学习地址。远程管理交换机时，请将您的管理终端的 MAC 地址或网关 MAC 地址作为静态地址加入到交换机中，以预防在某些情况下失去对交换机的远程管理能力。

本页对动态地址绑定进行配置，包括以下设置（如下图）：

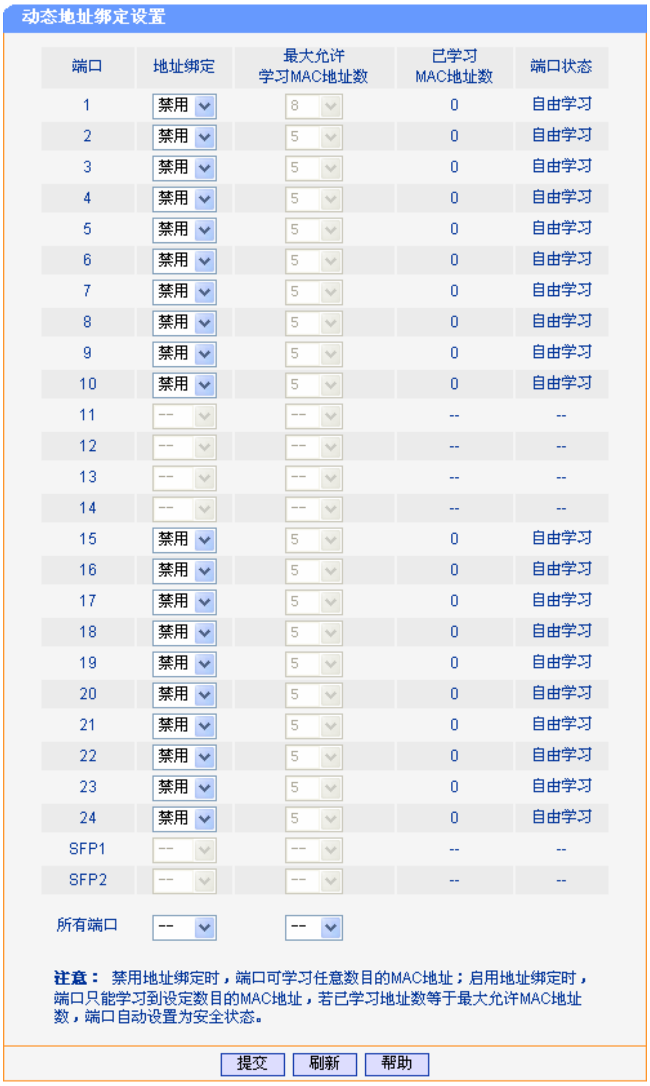


图 4-31 动态地址绑定设置

地址绑定： 地址绑定有三种状态："禁用"、"启用" 和 "--"。

- 禁用：将当前端口设置为自由学习状态。
- 启用：将当前端口设置为地址绑定状态。当端口绑定地址数目达到最大值后，端口将自动变成安全端口，不再学习新的 MAC 地址。
- -- ：只有当前端口为安全端口的时候，才会出现该选项。选择该项表示保持该端口为安全端口不变。

最大允许学习 MAC 地址数： 只在地址绑定功能启用时才生效，用来设定对应端口最多可以学习的 MAC 地址数目。

已学习 MAC 地址数: 只在地址绑定功能启用时才有意义，显示在交换机的动态绑定 MAC 地址表中本端口已经学习到的 MAC 地址数目。

端口状态： 共有五种状态，自由学习、学习中、安全端口、未初始化和 "--"。

- 自由学习：表示动态 MAC 地址绑定功能被禁止，端口可以自由学习 MAC 地址，没有数目限制。
- 学习中：表示端口当前处于动态地址绑定状态，但是学习到的 MAC 地址数目小于"最大允许学习 MAC 地址数"，仍然可以学习新的 MAC 地址。
- 安全端口：表示端口根据"最大允许学习 MAC 地址数"规定的数目，

已经学习满了，或者是在端口管理的"端口参数"页中，用户已将这个端口手动设置为安全端口。

- 未初始化：意思是说扩展插槽的位置仍然空出，没有使用扩展模块。

注意：

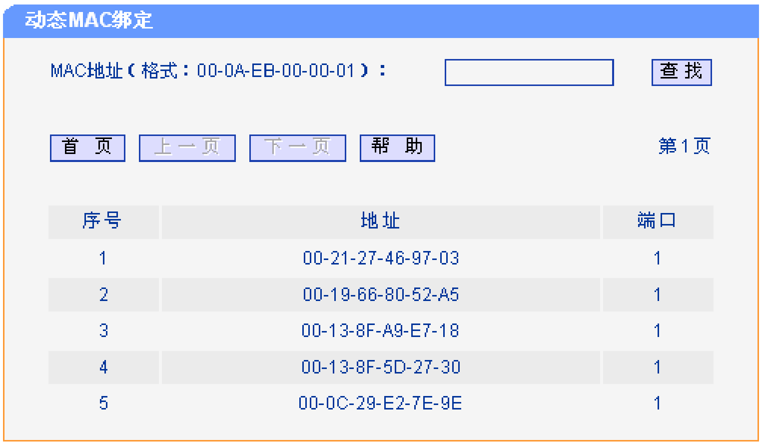
1. 当端口为 Trunk 成员，或者是未插装的扩展插槽位时，端口的地址绑定功能被禁用。只有将端口从 Trunk 组中去掉，或者将模块插入扩展槽位后，才可以使用端口的动态地址绑定功能。
2. 在端口的地址绑定功能被禁止或者交换机重启后，绑定的 MAC 地址将被删除。
3. 若 802.1X 模块开启，此功能禁用。

说明：

1. 若在"端口参数"页面中手动将端口设置为安全端口时，端口的动态地址绑定功能不能被启用或禁用；若端口启用了动态地址绑定，并且由于学习满后自动变成了安全端口，则可以在此页中再次启用或禁止端口的动态地址绑定功能。
2. "所有端口"后的两个下拉框用以同时改变所有端口的地址绑定状态和最大允许 MAC 地址学习数。
3. 页面提供"刷新"键，您可以通过此键查看最新的 MAC 地址绑定数。

4.3.5 动态MAC绑定

本页对动态绑定 MAC 地址进行查看。包括以下状态（如下图）：



序号	地址	端口
1	00-21-27-46-97-03	1
2	00-19-66-80-52-A5	1
3	00-13-8F-A9-E7-18	1
4	00-13-8F-5D-27-30	1
5	00-0C-29-E2-7E-9E	1

图 4-32 动态绑定 MAC 地址

MAC 地址： 输入要查找的 MAC 地址，参考格式为 00-0A-EB-00-00-01。

查找： 查找需要的 MAC 地址所对应的条目。

地址： 显示已经被端口动态绑定到的 MAC 地址。

端口： 显示 MAC 地址对应的交换机端口。

注意：

若 802.1X 模块开启，此功能禁用。

4.4 系统工具

TL-SG2224P 交换机将管理交换机的常用系统工具组合在一起，为您定位并排除网络故障提供了便捷的方法。在系统工具中，您可以直接对交换机进行重启和复位，通过 ping 检测功能检测交换机局域网中的计算机是否正常运行，线缆检测功能进行局域网中的线缆检测，还可以通过 LOG 信息查看所有交换机上的配置并找出错误配置。

点击**系统工具**，您可以看到：



4.4.1 重启和复位

交换机的一些功能配置，除了需要提交保存配置以外还需要重启才能使配置生效。如果需要同时改变交换机的绝大多数配置则可以通过“复位”键来使交换机软件复位后重新设置。本页对重启和复位进行配置，包括以下设置（如下图）：

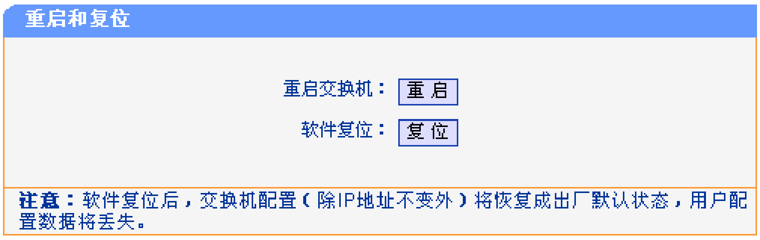


图 4-33 重启和复位

注意：

软件复位后，交换机配置（除 IP 地址不变外）将恢复成出厂默认状态，用户配置数据将丢失。交换机出厂设置表请参见附录 C。

4.4.2 ping检测

Ping 检测和普通计算机上的 ping 命令一样，都是用来检测网络中两个节点之间的链路是否连通。两者区别在于，两台普通计算机之间的 ping 命令是为了检测物理链路连接是否正常，而交换机的 ping 检测功能是为了方便网络管理员检测局域网中的网络设备是否已经断开连接，定位网络故障。

本页对 ping 检测行配置，包括以下设置（如下图）：



图 4-34 Ping 检测

目标 IP 地址： 测试的目的节点的 IP 地址。

发送次数： 设置发起 ping 检测时发送的 ping 报文次数。建议使用缺省值。

发送报文长度： 设置发起 ping 检测时 ping 报文长度。建议使用缺省值。

时间间隔： 发起 ping 检测时，若没有收到回复，则在配置的时间间隔后再发送 ping 报文，直到所发送的报文数达到所设置的发送次数。

4.4.3 线缆检测

TL-SG2224P 提供了线缆检测功能。当交换机端口连接有合适的双绞线时，您可以通过交换机对双绞线的状态进行测试，确认有无问题，以及发生问题的地方。此功能对于日常工程安装诊断有一定参考价值。

本页对线缆检测进行配置，包括以下设置（如下图）：



图 4-35 电缆检测

检测端口： 选定要检测的双绞线所连接的端口。

线路状态： 端口连接的以太网双绞线的状态。可能显示的状态有：正常、短路、开路、阻抗失配。另外还可能出现线路不支持检测或检测失败的情况。

- 开路：指线路中有断开现象，造成这种情况的原因一般是水晶头处线缆接触不良，一般用线缆测试设备能进行故障点定位。
- 短路：指线路中有一根或多根线金属内芯互相接触，导致短路；连接在 100M 模式或者网线坏的。
- 阻抗失配：网线质量好坏，接头好坏等，归根为网线的质量。

线路长度： 若线路为正常状态，则可检测出该线路的长度范围。线缆检测支持的最大线长是 170 米。此外，如果正常连接的线长小于 30 米或者大于 140 米，也会导致线长检测的结果不准确。

出错长度： 若线路为短路、开路或阻抗失配状态，则可检测出该线路的出错长度（即线路上出错点到端口一端之间的距离）。

检测： 选定检测端口后，点击“检测”键进行线路检测。

注意：

1. 这里的长度是指线缆绕对的长度，并不是线缆表皮的长度。因为一般来说绕对的长度要比表皮的长度长，并且 4 对绕对的线缆可能长度不一，每对线对的绞率不同。一般线缆检测显示的长度会有较大误差。
2. 检测结果仅供参考，特殊的情况也可能会检测错误或失败。

4.4.4 系统日志

TL-SG2224P 交换机提供的日志系统能够对所有的系统信息进行记载、分类、管理，为网络管理员监控设备运行情况和诊断设备故障提供强有力的支持。点击“刷新”键可以查看交换机的系统日志。下图为系统刚开机后的系统日志。



图 4-36 系统日志

TL-SG2224P 系统信息格式:【时间/模块名/信息级别:信息文本】，可以看出日志信息具有以下一些特性:

时间: 相应设置发生的时间。

模块名: 相应设置所属功能模块。

信息级别: 说明该条配置信息的严重等级，共分为 1-7 级，如下表所示。

信息文本: 描述该条配置信息的具体内容。

级别名称	等级	描述
SL_EMERGENCIES	1	系统不可用信息
SL_CRITICAL	2	严重信息
SL_ERRORS	3	错误信息
SL_WARNINGS	4	警告信息
SL_NOTIFICATIONS	5	正常出现但是重要的信息
SL_INFORMATIONAL	6	需要记录的通知信息
SL_DEBUGGING	7	调试过程产生的信息

第5章　高级功能模块

TL-SG2224P 交换机的高级功能包括 **VLAN 管理**、**ARP 攻击防护**、**网络优化**、**服务质量（QoS）** 以及 **802.1X 认证**五个部分。

5.1 VLAN管理

5.1.1 VLAN简介

VLAN（Virtual Local Area Network）即虚拟局域网，是一种通过将局域网内的设备逻辑的而不是物理的划分成一个个局域网从而实现虚拟工作组的技术。VLAN 把一个物理上的 LAN 划分成多个逻辑上的 LAN，每个 VLAN 是一个广播域。同一个 VLAN 内的主机间通过传统的以太网通信方式即可进行报文的交互，而处在不同 VLAN 内的主机之间如果需要通信，则必须通过路由器或三层交换机等网络层设备才能够实现。

5.1.1.1 VLAN技术产生的背景

传统的以太网是广播型的网络，网络中的所有主机处在同一个广播域中，它们之间通过 HUB 或交换机相连。HUB 即集线器是物理层设备，没有交换功能，接收到报文之后会向除接收端口外的所有端口转发；交换机是数据链路层设备，具备根据报文的目的 MAC 地址进行转发的能力，但在收到广播报文或未知单播报文（报文的目的 MAC 地址不在交换机 MAC 地址表中）时，也会向除接收端口之外的所有端口转发。这样就会造成以下网络问题：

- 网络中可能存在着大量广播报文和未知单播报文，浪费网络资源。
- 网络中的主机收到大量并非以自身为目的地的报文，造成了严重的安全隐患。

如果整个网络只有一个广播域，那么一旦发出广播信息，就会传遍整个网络，消耗网络整体带宽，并且对网络中的主机带来额外的负担。因此 VLAN 的技术应运而生，划分 VLAN 以后，数据只会在自己所属的 VLAN 内广播从而实现广播域的划分。

5.1.1.2 VLAN的优点

了解了划分 VLAN 的原因以及 VLAN 的概念，在这总结一下 VLAN 的几个优点：

- 控制网络的广播风暴

限制广播在 VLAN 内，而不是整个局域网，从而有效控制网络的广播风暴，避免了网络资源的浪费。

- 增强网络安全

不同 VLAN 的设备不能互相访问，各个 VLAN 内的主机间不能直接通信，需要通过路由器或三层交换机等网络层设备对报文进行三层转发

- 简化网络管理

逻辑上的划分，而不是物理上。因此同一个虚拟工作组的主机不会局限在某个物理范围内，简化了网络的管理，方便了不同区域的人建立工作组。

5.1.2 VLAN的类型及工作原理

根据 VLAN 划分方式的不同产生了不同的 VLAN 类型，TL-SG2224P 交换机的 VLAN 类型主要包括：Port VLAN、Tag VLAN 和 MTU VLAN。此款交换机可以选择不设置 VLAN、基于端口的 VLAN 模式、IEEE 802.1Q Tag VLAN 模式或 MTU VLAN 模式。

- 不设置 VLAN 时，交换机无任何 VLAN，任何数据包都可以在交换机上任意端口之间转发。
- Port VLAN 是基于端口的 VLAN。处于同一 VLAN 的端口之间才能相互通信，这样可有效地屏蔽广播风暴，并提高网络安全性能。由于端口 VLAN 具有实现简单，易于管理的优点，所以适用于连接位置比较固定的用户。下图是 Port VLAN 示意图：

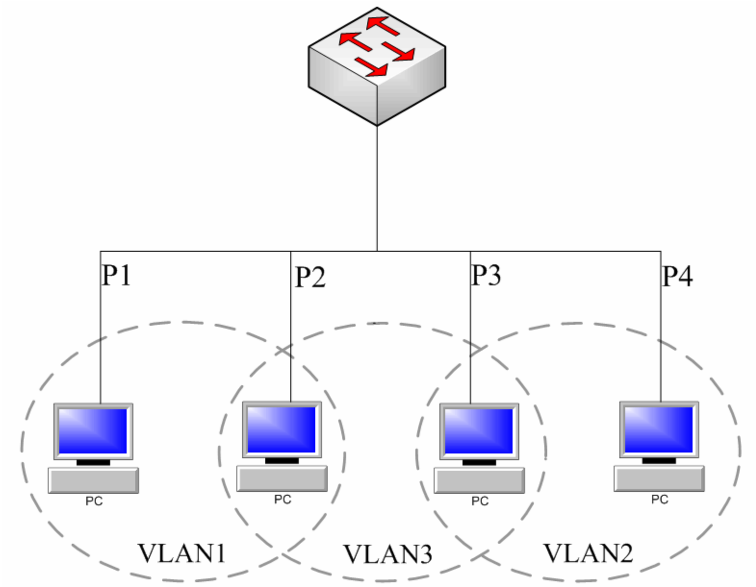


图 5-1 Port VLAN 示意图

- IEEE 802.1Q Tag VLAN 是基于 IEEE 802.1Q 协议的 VLAN 划分方法。下图是 Tag VLAN 的组网示意图：

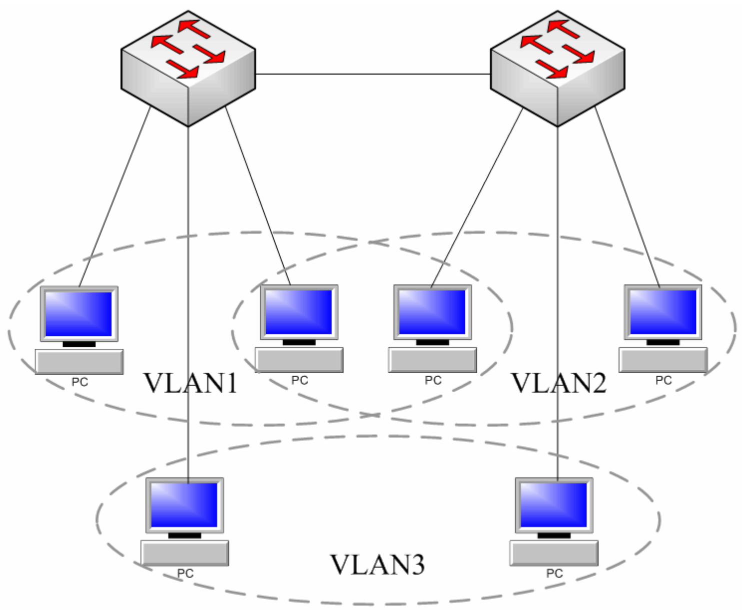


图 5-2 Tag VLAN 组网示意图

在 VLAN 最初被应用时，各厂商的交换机由于缺乏统一标准而互不识别，无法兼容。于是，IEEE 802.1Q 这一新的虚拟局域网标准被制订出来，使不同厂商的设备可同时在同一网络中使用。只要符合 IEEE 802.1Q 标准的交换机就可以相互通信。

IEEE 802.1Q 标准定义了一种新的帧格式，它在标准的以太网帧的源地址后面加入了一个 Tag 头，如图所示：

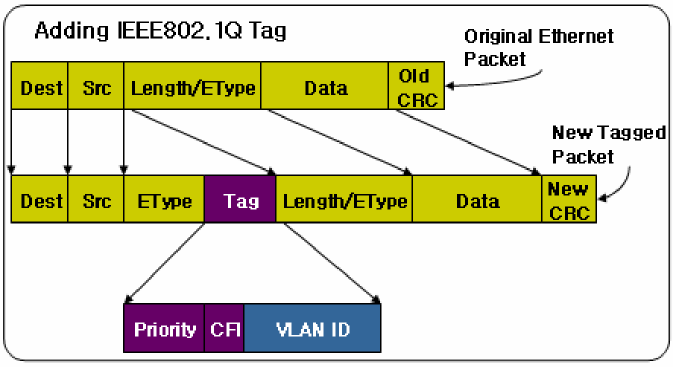


图 5-3 IEEE 802.1Q 帧格式

基于 IEEE 802.1Q 的 Tag VLAN 用 VID 来划分不同的 VLAN，当数据帧通过交换机的时候，交换机根据帧中 Tag 头的 VID 信息来识别它们所在的 VLAN，这使得所有属于该 VLAN 的数据帧，不管是单播帧、多播帧还是广播帧，都将限制在该逻辑 VLAN 中传播。工作组中主机之间能够相互彼此通信，而不受其它主机的影响，就像它们存在于单独的局域网当中一样。

说明:

若帧中无 Tag 头，我们称这种帧为 Un tag 帧，并使用帧所通过交换机端口的缺省 VID 信息来识别它们所在的 VLAN。还可以通过设置交换机，对 Un tag 帧进行不同的处理。

- MTU VLAN（Multi-Tenant Unit VLAN）是将每个用户所占用的端口与上联端口划分为一个单独的 VLAN。普通端口只能和预先设置的上联端口进行通信，相互之间无法通信即不同端口的用户之间不能直接通信，保障网络的安全。这种情况很适合使用在智能小区中，用户之间不可以直接访问，从而保证住户的网络安全。以下是 MTU VLAN 的示意图：

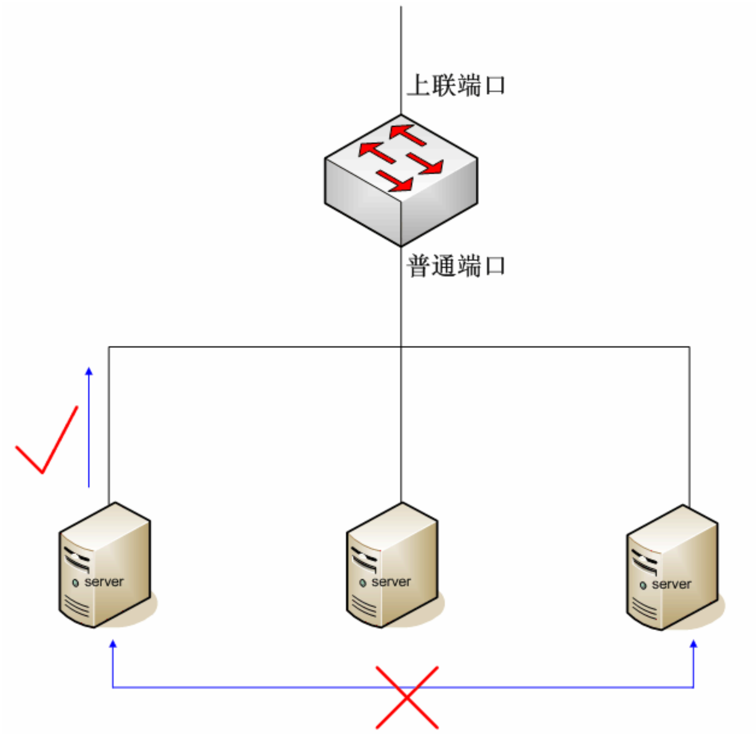
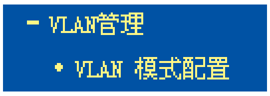


图 5-4 MTU VLAN 示意图

5.1.3 WEB界面配置

点击 **VLAN** 管理，您可以看到：



5.1.3.1 VLAN模式配置

本页对 VLAN 模式进行配置。包括以下设置（如下图）：



图 5-5 VLAN 模式配置

不设置 VLAN：	交换机不配置 VLAN，所有端口之间都可以互通。
Port VLAN：	即基于端口的 VLAN，配置的 VLAN 基于交换机的物理端口。
Tag VLAN：	即 802.1Q Tag VLAN，配置的 VLAN 基于 IEEE802.1Q 协议。
MTU VLAN：	在某些情况下我们需要交换机上的工作端口互相不能访问，只和上行口之间可以互通，这时可以选择这种模式。

注 意：

若当前设置有 Trunk 口，则不能设置为 MTU VLAN 模式。

5.1.3.2 Port VLAN配置

本页对 Port VLAN 进行配置，只有在选择 Port VLAN 模式下才显示。包括以下设置（如下图）：



图 5-6 Port VLAN 配置

VLAN 号：	VLAN 的编号，在这里选择一个 VLAN 号将跳转到该 VLAN 的配置页面。可设的 Port VLAN 数目与交换机的总端口数相同。
端口：	该列的数字即对应与交换机的物理端口。
成员：	勾选该 VLAN 的端口成员。
端口描述：	显示相应的端口描述信息。
查看所有：	点击后可以弹出下图所示窗口，显示了当前已设置的所有 VLAN 及其成员的列表。



图 5-7 查看已设 Port VLAN

基于端口的 VLAN 配置规则：

1. 新建立的或修改的 VLAN 不能是已存在的 VLAN 的父集或子集。
2. 不能设置一个空的 VLAN 且 VLAN 成员不能少于两个（页面上提交一个成员为空的 VLAN 表示删除该 VLAN）。

说明：

1. Trunk 口可作为一个逻辑端口参与 VLAN 的配置。图 5-6 中的 “T1”、“T2” 表示 Trunk，当设有 Trunk 时，Trunk 的成员端口对应的复选框不可选，而相应 Trunk 的复选框可以选择，反之亦然。交换机的千兆口和扩展模块口都可以作为 VLAN 成员参与配置。

2. 刚启用 Port VLAN 模式时默认设置了一个包含所有可选端口的 Port VLAN（VLAN 号为 1）。
3. 没有设置 VLAN 的端口，交换机会自动地把这几个端口设置到同一 VLAN 中。
4. 要删除一个已设置的 VLAN，请在“VLAN 号”一栏选择 VLAN 号跳转到该 VLAN 的配置页面，按“清空”键将所有“成员”复选框清空，然后按“提交”即可。
5. 基于端口的 VLAN 可设置条目数是与该交换机的端口数相等的。

5.1.3.3 Tag VLAN全局配置

全局配置是指这里的配置针对交换机的所有端口而不是具体的 VLAN，对每一个在后面设置的 VLAN 都有影响。

本页对 Tag VLAN 进行配置，只有在选择 Tag VLAN 模式下才显示。包括以下设置（如下图）：



图 5-8 Tag VLAN 全局配置

缺省 VID： 当交换机接收到一个没有 Tag 头(Un tag)的帧时，交换机将会自动地给该帧加一个 Tag 头，其 VID 就是该帧所进入交换机的那个端口的缺省 VID。

Un tag 帧处理： 当端口接收到的数据帧没有 Tag 头时的处理方式。可选项为“丢弃”和“通过”，如果选择“丢弃”则交换机会丢弃没有 Tag 头的数据帧，如果选择“通过”则交换机会将此帧在端口缺省 VID 对应的 Tag 值的那个 VLAN 里面转发。

说明：

图 5-8 中的“T1”、“T2”表示 Trunk，当设置有 Trunk 时，则此 Trunk 的成员端口将不能配置且显示的参数是其所属 Trunk 的参数。

5.1.3.4 Tag VLAN配置

与前面的全局设置不同，本页分别对每个 VLAN 进行设置，各个 VLAN 互不影响，但他们都受全局设置的影响。其设置如下图：

本页对 Tag VLAN 进行配置，只有在选择 Tag VLAN 模式下才显示。包括以下设置（如下图）：

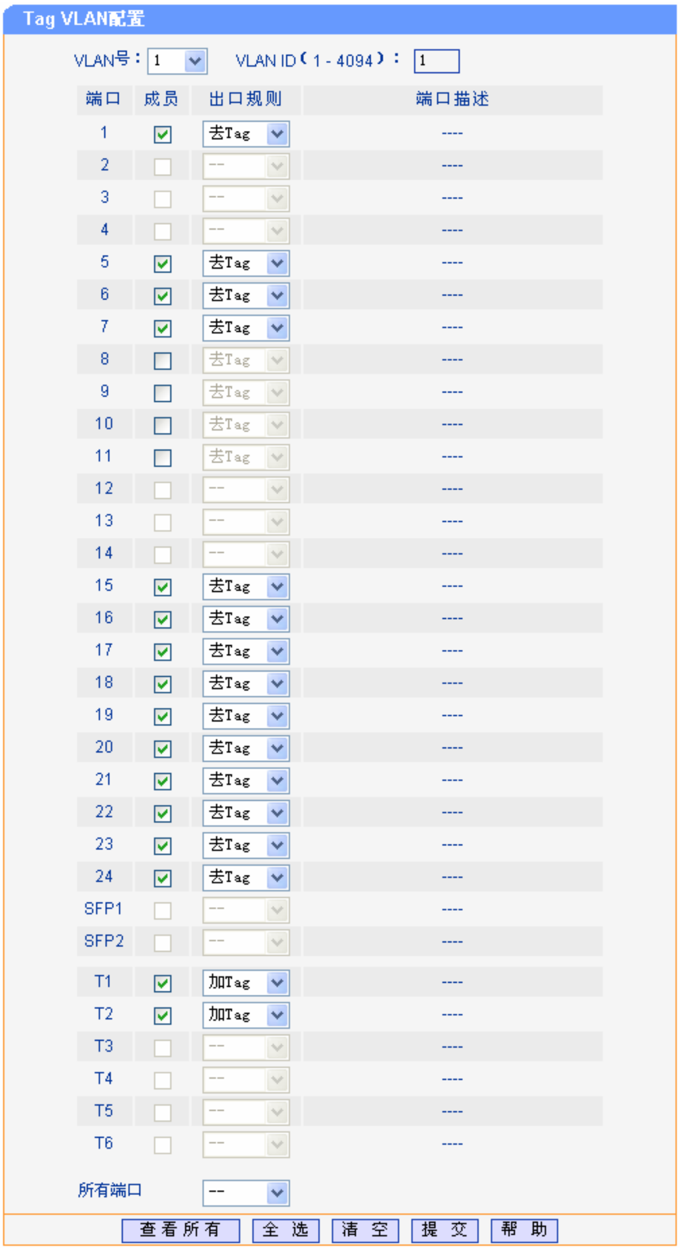


图 5-9 Tag VLAN 配置

VLAN ID： 即配置 Tag VLAN 的时候 VLAN 的全局标签值。

出口规则： 对数据帧的处理方式。“去 Tag”表示从该端口发出的数据帧不带 Tag 字段；“加 Tag”表示从该端口发出的数据帧包含 Tag 字段。

查看所有： 键点击后可以弹出下图所示窗口，显示了当前已设置的所有 VLAN 及其成员的列表。



图 5-10 查看已设 Tag VLAN

IEEE 802.1Q Tag VLAN 配置规则：

1. VLAN 的 VID 必须是唯一的。
2. VLAN 的合法 VID 必须在 1－4094 之间。
3. 不能设置一个空的 VLAN 且 VLAN 成员不能少于两个（页面上提交一个成员为空的 VLAN 表示删除该 VLAN）。
4. 如果端口连接的是不支持 IEEE 802.1Q 协议的设备（如 HUB 不支持 IEEE 802.1Q 协议的网络适配器时），只能将该端口的出口规则设置为“去 Tag”。

说明：

1. Trunk 口可作为一个逻辑端口参与 VLAN 的配置。图 5-9 中的“T1”、“T2”表示 Trunk，当设有 Trunk 时，Trunk 的成员端口对应的复选框不可选，而相应 Trunk 的复选框可以选择，反之亦然。交换机的千兆口和扩展模块口都可以作为 VLAN 成员参与配置。
2. 刚启用 Tag VLAN 模式时默认设置了一个包含所有端口的 Tag VLAN（VLAN 号为 1）。要删除一个已设置的 VLAN，请在“VLAN 号”一栏选择 VLAN 号跳转到该 VLAN 的配置页面，按“清空”键将所有“成员”复选框清空，然后按“提交”即可。
3. 某几个端口不属于任何 TAG VLAN 成员时，这几个端口之间不能相互通信（这点与基于端口的 VLAN 不同），也不能和任何 VLAN 成员端口相互通信。

5.1.3.5 MTU VLAN配置

本页对 MTU VLAN 模式进行配置，只有在选择 MTU VLAN 模式下才显示。包括以下设置（如下图）：

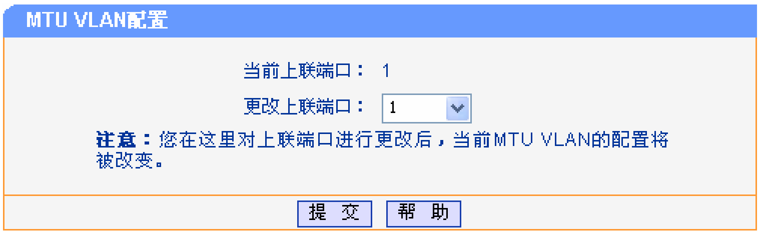


图 5-11MTU VLAN 配置

说明：

1. 当设置某个端口为上联端口时，它将依次和其余的端口分别组成一个 VLAN，每个 VLAN 包含两个端口：一个为刚才设置的上联端口，另一个依次为这个上联端口之外的其他端口。
2. 刚启用 MTU VLAN 模式时默认将端口 1 设置为上联端口。
3. 若当前配置了 Trunk，MTU VLAN 将不能配置。

5.2 ARP攻击防护

5.2.1 ARP简介

ARP（Address Resolution Protocol，地址解析协议）用于将网络层的 IP 地址解析为数据链路层的物理地址。

网络上的一台主机把以太网数据帧发送到位于同一局域网上的另一台主机时，是根据主机的数据链路层地址（包括 MAC 地址）进行转发的，设备驱动程序从不检查 IP 数据帧中的目的 IP 地址，所以需要将 IP 地址解析为数据链路层地址以保证主机之间的数据帧能够正常转发。

5.2.1.1 ARP表

以太网上的主机通信都需要知道对方的 MAC 地址，所以每台主机内部都维护着一张 ARP 表。其中记录了一些最近与本主机通信的其他主机的 MAC 地址与 IP 地址的对应关系。每一条 IP 地址与 MAC 地址映射关系称为一条 ARP 表项。

5.2.1.2 ARP地址解析过程

假设以一个主机 A 向同局域网内的主机 B 发送数据，地址解析过程如下：

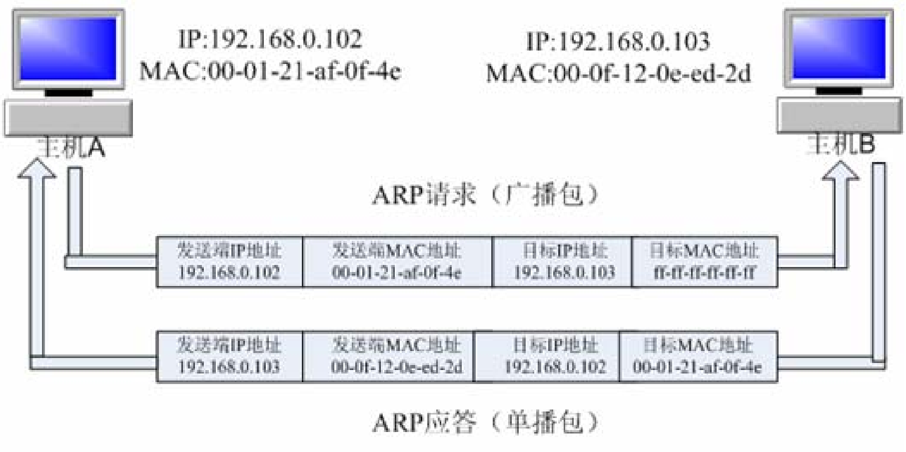


图 5-12 地址解析拓扑图

1. A 在自己的 ARP 表中查询是否存在主机 B 的 IP 地址和 MAC 地址的对应条目。若存在，直接向主机 B 发送数据。若不存在，则 A 向整个局域网中广播一份称为“ARP 请求”的数据链路帧，这个请求包含发送端（即主机 A）的 IP 地址和 MAC 地址以及接收端（即主机 B）的 IP 地址。
2. 局域网的每个主机接收到主机 A 广播的 ARP 请求后，目的主机 B 识别出这是发送端在询问它的物理地址，于是给主机 A 发出一个 ARP 应答。这个应答包含了主机 B 的物理地址。
3. 主机 A 接收到主机 B 发出的 ARP 应答后，就将主机 B 的 IP 地址与 MAC 地址的对应条目添加自己的 ARP 表中，以便后续报文的转发。

5.2.2 ARP欺骗原理

按照 ARP 协议的设计，一个主机也会接收不是自己主动请求的 ARP 应答，并将应答中的 IP 地址和物理地址添加到 ARP 表中，这样设计是为了减少网络上过多的 ARP 通信量，但同时也为“ARP 欺骗”创造了条件。

ARP 欺骗的方式有多种，包括中间人攻击、网关欺骗、主机欺骗等等。

5.2.2.1 中间人攻击

假设同一个局域网内，有 3 台主机通过交换机相连：

A 主机：IP 地址为 192.168.0.1，MAC 地址为 00-00-00-11-11-11；

B 主机：IP 地址为 192.168.0.2，MAC 地址为 00-00-00-22-22-22；

C 主机：IP 地址为 192.168.0.3，MAC 地址为 00-00-00-33-33-33。

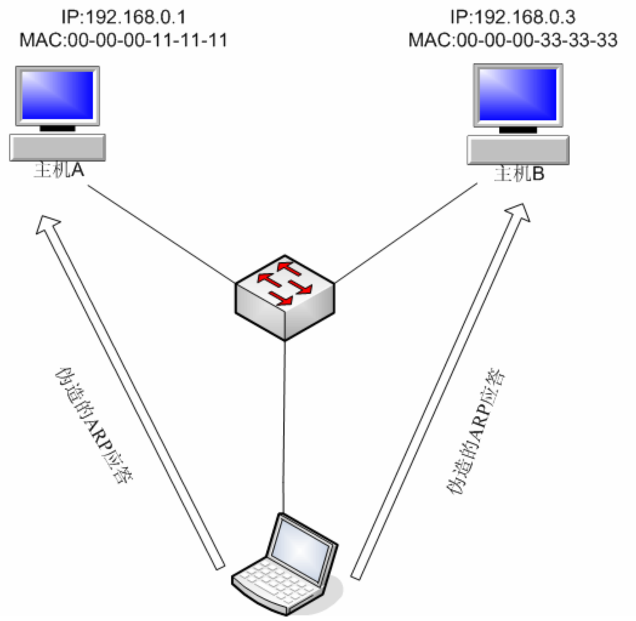


图 5-13 中间人攻击

B 主机对 A 和 C 进行欺骗的前奏就是发送假的 ARP 应答。A 在收到 B 主机发来的 ARP 应答后，A 主机应知道：到 192.168.0.3 的数据包应该发到 MAC 地址为 00-00-00-22-22-22 的主机；C 主机也知道：到 192.168.0.1 的数据包应该发到 MAC 地址为 00-00-00-22-22-22 的主机。这样，A 和 C 都认为对方的 MAC 地址是 00-00-00-22-22-22，实际上这就达到了 B 主机发起中间人攻击的目的。当然，因为 ARP 缓存表项是动态更新的，其中动态生成的映射有个生命期，一般是两分钟，如果再没有新的信息更新，ARP 映射项会自动去除。所以，B 还有一个“任务”，那就是连续不断地向 A 和 C 发送这种虚假的 ARP 响应包，让其 ARP 缓存中一直保持被毒害了的映射表项。

现在，如果 A 和 C 要进行通信，实际上彼此发送的数据包都会先到达 B 主机，这时，如果 B 不做进一步处理，A 和 C 之间的通信就无法正常建立，B 也就达不到“嗅探”通信内容的目的，因此，B 要对“错误”收到的数据包进行一番修改，然后转发到正确的目的地。而修改的内容，就是将目的 MAC 地址和源 MAC 地址进行替换。在 A 和 C 看来，彼此发送的数据包都是直接到达对方的，但在 B 来看，自己担当的就是“第三者”的角色。这种嗅探方法，也被称作“中间人”的方法。

5.2.2.2 网关欺骗

网关欺骗是指攻击者发送伪造的网关 ARP 报文，欺骗同网段内的其他主机。从而网络中同网段主机访问网关的数据被定义到一个错误的 MAC 地址，导致其他主机无法正常访问外网。

5.2.2.3 主机欺骗

主机欺骗是指攻击者冒充某网段内的一台主机，向网关发送伪造的 ARP 报文，通知网关该主机的 MAC 地址已经改变，使得网关更新自己的 ARP 表，从而网关发给该主机用户的数据被定义到一个错误的 MAC 地址，导致该主机用户将无法正常访问外网。

5.2.3 WEB界面配置

点击 **ARP 攻击防护**您可以看到：



5.2.3.1 全局配置

本页对 ARP 防护进行全局配置。包括以下设置（如下图）：



图 5-14 全局配置

您可以通过特殊端口的配置灵活控制 ARP 报文的检测功能。对于来自特殊端口的 ARP 报文是不需要检测的，例如上联端口、路由端口以及交换机管理端口等都是需要被设为特殊端口的。而对来自其它端口的 ARP 报文，需要查看报文中的源 IP 地址，源 MAC 地址和进入交换机的端口三者绑定关系与 ARP 信任条目表项是否一致。若一致，则为合法报文，进行转发处理，否则将予以丢弃。因此，在开启 ARP 防护之前，应先配置 ARP 信任条目，以免影响正常通信。

ARP 防护： 选择"禁用"，关闭 ARP 防护功能；选择"启用"，打开 ARP 防护功能。此项默认值为禁用。

特殊端口配置： 配置不需要进行 ARP 防护的端口。

5.2.3.2 主机绑定

本页对主机绑定进行配置。包括以下设置（如下图）：



图 5-15 主机绑定

您可以手动将某个主机的 MAC 地址、IP 地址以及与交换机连接的对应端口号进行绑定作为一个信任条目。对于接收到的来自非信任端口的 ARP 报文，交换机将查看报文中的 IP 地址、MAC 地址以及端口号的绑定关系是否与信任条目一致。若一致，则转发处理报文，否则丢弃。

当前状态： 分为“启用”和“禁用”。

状态更改：

- 启用/禁用：使当前状态更改为启用或禁用。
- 编辑：可以对主机描述、MAC 地址、IP 地址进行编辑。
- 删除：删除当前绑定。

不仅如此，您还可以通过主机扫描，自动探测某个网段中主机的 MAC、IP、PORT 对应关系，您只需要从中选择您需要的绑定条目添加到您的信任条目中。同时当侦测结果中有两个或以上条目拥有同一个 IP 地址或 MAC 地址时，网络中可能存在 ARP 欺骗，该条目会以红色报警显示。此时您可以对探测处理的信息条目进行分析，并对得到的非法条目进行处理，排除内部网络隐患。

> **注意：**
>
> 主机扫描可以侦测出直接连接在交换机下的所有主机，但对于通过其他交换机级联的主机，侦测到的数目与其 VLAN 的设置有关。

主机扫描界面如下：



网络主机探测

扫描范围设定

起止IP地址：

需要扫描的端口：

1	2	3	4	5	6	7	8	9	10	11	12
☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
13	14	15	16	17	18	19	20	21	22	23	24
☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

扫描

扫描结果

ip地址	mac地址	端口	选定
192.168.0.1	00-0A-EB-00-13-01	10	☐
192.168.0.5	00-19-66-80-54-49	10	☐
192.168.0.23	00-19-E0-00-01-9A	10	☑
192.168.0.78	00-19-66-80-54-36	1	☐
192.168.0.82	00-19-66-80-54-49	10	☐
192.168.0.84	00-19-66-80-53-DE	10	☐
192.168.0.92	00-19-66-80-54-2B	10	☐
192.168.0.100	00-19-66-64-ED-29	10	☐

全选　清空　绑订选中项　返回　帮助

图 5-16 网络主机探测

起止 IP 地址： 确定您需要探测的 IP 地址段。

需要扫描的端口： 默认为全部端口，当然您可以根据您的需要勾选。

扫描： 探测以上设置的 IP 地址段内、端口上的 IP 地址、MAC 地址、端口对应关系。

绑定选中项： 将您选定的一项作为绑定的信任条目。

5.2.3.3 非法ARP统计

交换机会对所有端口的非法 ARP 包进行统计。当非法的 ARP 报文速率超过交换机内部设定的阈值时，页面上会以红色突出显示，此时您只需对相应的端口下的计算机进行排查。本页对非法 ARP 统计进行配置。包括以下设置（如下图）：

非法ARP统计

端口	非法ARP包	特殊端口	端口	非法ARP包	特殊端口
1	450	否	2	0	否
3	0	否	4	0	否
5	1816	否	6	0	是
7	96	否	8	0	否
9	0	否	10	0	否
11	0	否	12	0	否
13	0	否	14	0	否
15	0	否	16	132	否
17	0	否	18	0	是
19	118	否	20	0	否
21	0	否	22	0	否
23	0	否	24	0	否

刷 新　清 零　帮 助

图 5-17 非法 ARP 统计

端口： 检测的端口号。

非信任 ARP 包： 统计的非信任 ARP 包的数目。

特殊端口： 显示该端口是否为特殊端口。

5.2.4 ARP组网应用

5.2.4.1 组网需求

现有交换机 TL-SG2224P IP：192.168.0.1；主机 A IP：192.168.0.34，MAC 地址：00-00-00-11-12-13；主机 B IP：192.168.0.64，MAC 地址：00-00-00-14-15-16。

TL-SG2224P 端口 1 连接上联交换机，端口 2，3 分别连接主机 A、主机 B，要求实现 ARP 绑定，在局域网中杜绝 ARP 攻击。

5.2.4.2 组网图

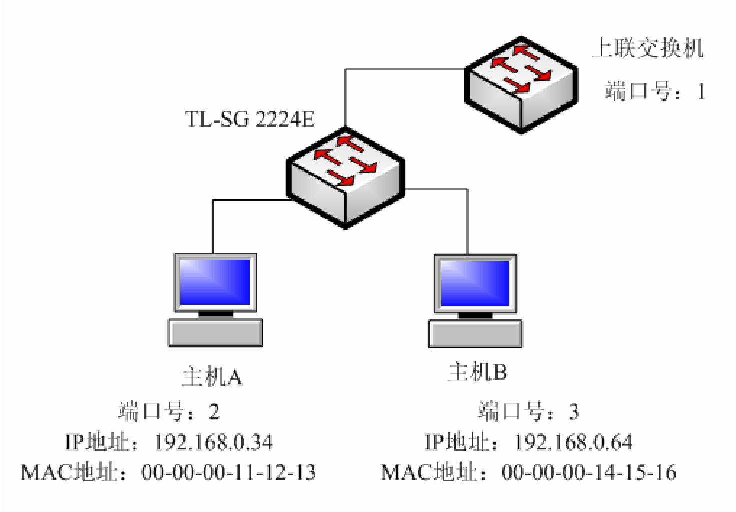


图 5-18 组网图

5.2.4.3 组网步骤

1. 将主机 A、B 的 IP 地址、MAC 地址以及端口号进行绑定添加进信任条目。有手动和主机扫描两种方式实现。

手动配置，界面如下：



将主机 A、B 的信息添加进绑定列表。

主机扫描，界面如下：



设置起止 IP 地址为：192.168.0.30---192.168.0.100,点击扫描。在扫描结果中选择主机 A 和主机 B 即可。

2. 因为上联交换机是可以信任的，所以将 1 端口添加进特殊端口，页面配置如下：



开启 ARP 攻击防护功能，将端口 1 选择为不需要进行 ARP 防护的端口，点击提交。

注意：

在开启 ARP 攻击防护功能之前需先绑定信任条目，否则可能会影响通信。

5.3 网络优化

5.3.1 组播概述

在网络中，存在着三种发送报文的方式：单播、广播、组播。采用单播（Unicast）方式时，服务器必须为每一个接收者传输一份信息，如果有多个接收者存在，网络上就会重复地传输多份相同内容的信息，占用了大量资源。如果采用广播（Broadcast）方式，系统把信息传送给网络中的所有用户，不管他们是否需要，任何用户都会接收到广播来的信息。

在 Internet 上，诸如视频会议和视频点播等单点发送、多点接收的多媒体业务正在成为信息传送的重要组成部分。在一点发送多点接收的前提下，单播方式适合用户较少的网络，而广播方式适合用户稠密的网络，当网络中需求某信息的用户量不确定时，单播和广播方式效率很低。这时组播（multicast）应运而生，它的出现提供了解决一个主机向特定的多个接收者发送消息的方法。如图 5-19 所示。

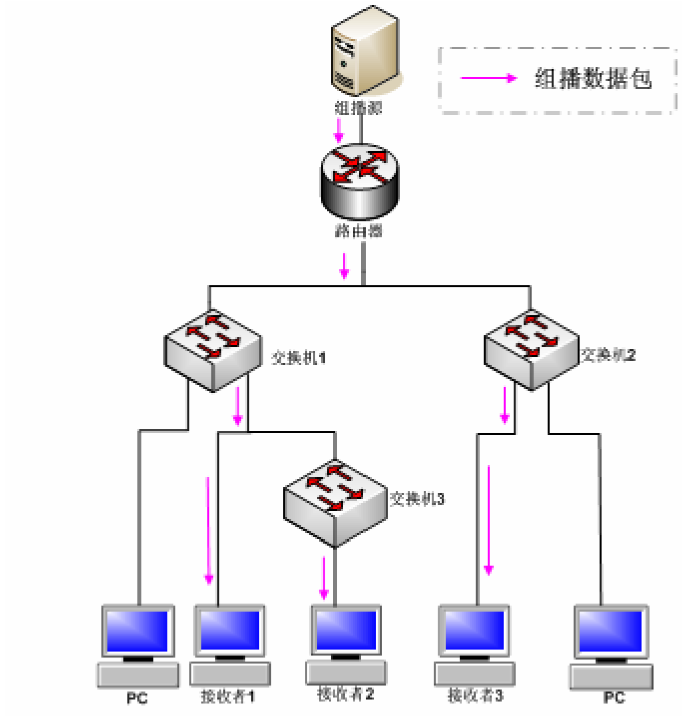


图 5-19 组播传输信息的方式

组播的特点是：服务对象不固定；通常是一对多的关系；把服务对象看成一个组，发送端只需要发送一次数据到相关网络设备即可；每个用户可以随时加入或退出该组；实时性要求较高；允许一定的丢帧现象发生等。

5.3.2 IGMP Snooping简介

IP 主机通过 IGMP（Internet Group Management Protocol，互联网组管理协议）协议向临近的路由器申请加入（或离开）组播组。IGMP Snooping（IGMP 侦听）是组播约束机制，通过侦听和分析主机与组播设备之间交互的 IGMP 报文来管理和控制组播组。

5.3.3 IGMP Snooping原理

5.3.3.1 IGMP Snooping的工作过程

IGMP Snooping 的工作过程是：交换机侦听用户主机与路由器之间的交互报文，跟踪组播信息及申请的端口。当交换机侦听到主机朝路由器发出的 IGMP Report(请求)报文时，交换机便把该端口加入组播转发表中；当交换机侦听到主机发送的 IGMP Leave（离开）报文时，路由器会发送该端口的 Group-Specific Query（特定组查询）报文，若其它主机需要该组播，则将回应 IGMP Report 报文，若路由器收不到任何主机的回应，交换机便把该端口从组播转发表中删除。路由器会定时发 IGMP Query（查询）报文，交换机收到 IGMP Query 报文后，如果在一定的时间段内没有收到主机的 IGMP Report 报文，便把该端口从组播表中删除。

5.3.3.2 IGMP Snooping相关端口

IGMP Snooping 的相关端口如图 5-20 所示，路由器连接组播源，在交换机 1、交换机 2 和交换机 3 上运行 IGMP Snooping，接收者 1、接收者 2 和接收者 3 为接收者主机（即组播组成员）。

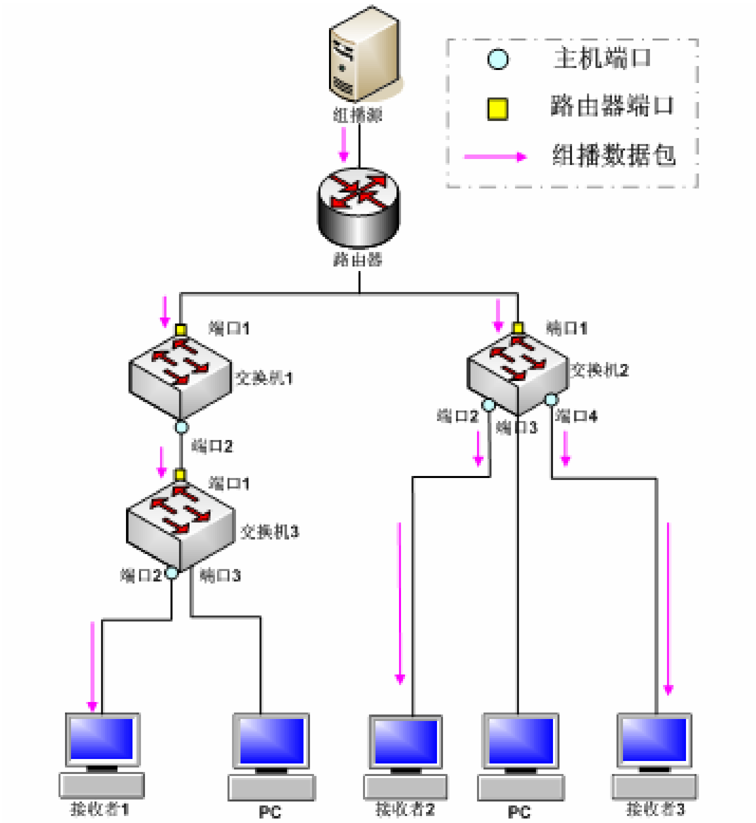
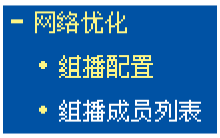


图 5-20 IGMP Snooping 相关端口

- 路由器端口（Router Port）：交换机上靠近三层组播设备一侧的端口。如交换机 1、交换机 2、交换机 3 中的端口 1。
- 主机端口（Member Port）：又称组播组成员端口，表示交换机上靠近组播组成员一侧的端口。如交换机 1 的端口 2、交换机 2 的端口 2 和端口 4、交换机 3 的端口 2。

5.3.4 WEB界面配置

点击**网络优化**您可以看到：



5.3.4.1 组播配置

本页对 IGMP 侦听进行配置。包括以下设置（如下图）：

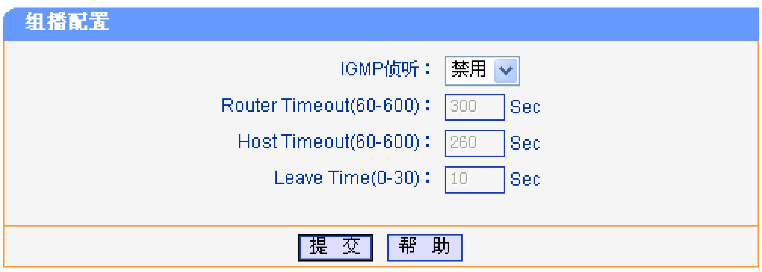


图 5-21 组播配置

IGMP 侦听： 全局启用或者禁用 IGMP 侦听功能。

Router Timeout： 路由器端口失效时间。这段时间内，如果交换机没从路由器端口接收到查询报文，就认为该路由器端口失效。默认是 300 秒。

Host Timeout： 主机端口失效时间。这段时间内，如果交换机没接收到主机端口发送的 report 报文，就认为该主机端口不再有主机属于多播组。默认是 260 秒。

Leave Timeout： 离开时间。主机发送离开报文到交换机把该主机端口从多播组中删除的间隔时间。默认是 10 秒。

当“VLAN 管理”中开启“TAG VLAN”时，组播配置会出现如下界面：



图 5-22 组播配置

Tag VLAN 设置： 可以选择在每个 Tag VLAN 里启用或者禁用 IGMP Snooping 功能。

注意：

1. 路由端口失效时间以及主机端口失效时间至少大于 2 倍的 IGMP 查询报文时间。
2. 若已经开启了 IGMP Snooping 功能，则不能设置 PORT VLAN 或者 MTU VLAN！有关 VLAN 的介绍请参见第 5.1 节。

5.3.4.2 组播成员列表

本页显示组播成员信息（如下图）。



图 5-23 组播成员列表

条目： 组播组编号。

IP： 组播组的 IP 地址。

组成员： 参加组播组的端口号。

5.3.5 组网应用

5.3.5.1 组网需求

对比交换机开启 IGMP 侦听功能前后局域网中组播数据包的发送情况。如下图：

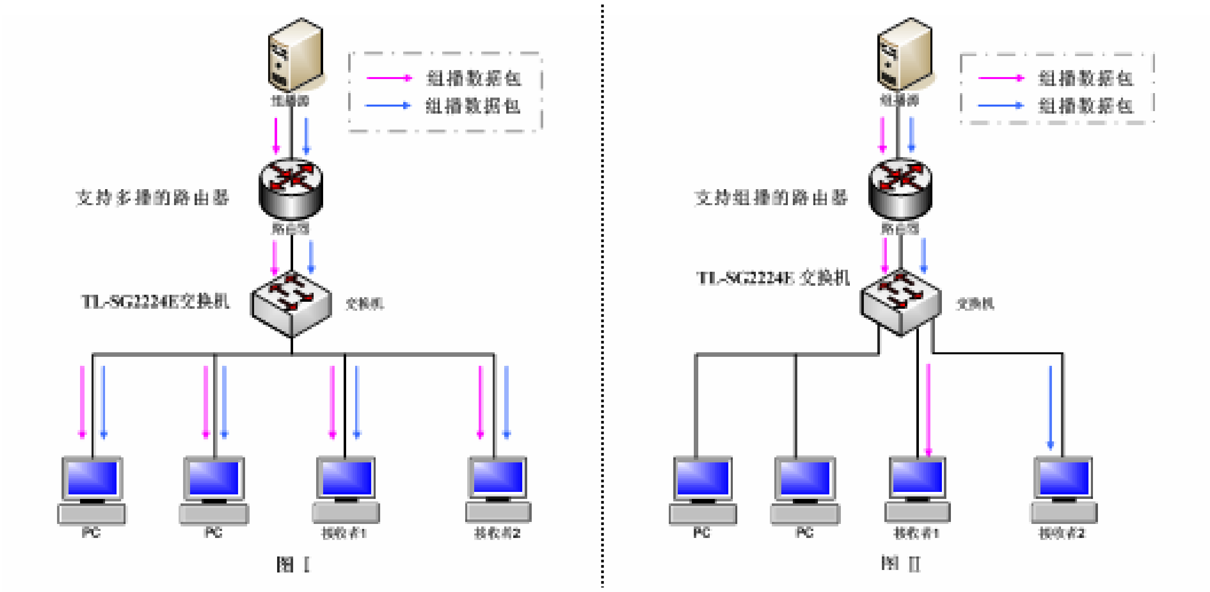


图 5-24 IGMP 侦听组网应用

TL-SG2224P 交换机上联一个支持组播功能的路由器，接收者 1、接收者 2 为接收者主机（即组播组成员），但是他们属于不同的组播组。图 I 中交换机的 IGMP 侦听功能未开启，图 II 中开启了 IGMP 侦听功能。

5.3.5.2 对比结果

图 I 中 IGMP 功能未开启，组播数据在局域网中被广播，大量无用的组播数据可能堵塞网络，造成网络的瘫痪。

图 II 中开启了 IGMP 侦听功能，组播数据会直接发送给指定的接收者，交换机的 IGMP 侦听功能起到了管理和控制组播数据的作用，从而减轻了网络负担。

5.4 服务质量QoS

5.4.1 QoS概述

QoS（Quality of Service）即服务质量，在 Internet 中用来表征网络服务的好坏。通常所说的 QoS，是针对各种网络应用的不同需求，为其提供不同的服务质量，如提供专用带宽，减少报文丢失率，降低报文传送时延及时延抖动等。即在带宽不充裕的情况下，对各种服务流量占用带宽的矛盾做一个平衡。

TL-SG2224P 交换机通过在入口阶段对数据流进行分类，然后在出口阶段将不同类型的数据流映射到不同优先级的队列，最后依据调度模式来决定不同优先级队列的数据包被转发的方式，从而实现了 QoS 功能。

5.4.2 QoS的相关原理

5.4.2.1 优先级模式

优先级模式：TL-SG2224P 交换机共有基于端口的优先级、IEEE 802.1p 优先级和 DSCP 优先级三种模式。其中默认启用基于端口的优先级，其他两种优先级模式可供选择。

1. 基于端口的优先级。

端口优先级有八个优先等级，分别对应到出口队列的 TC 0-TC 7，表示从该端口接收到的所有数据帧都被指定为设定的优先级，其中 TC 0 对应最低优先级的队列，TC 7 对应最高优先级的队列。

2. 802.1p 优先级。

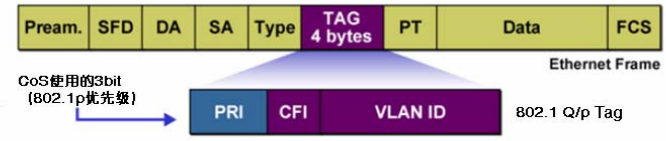


图 5-25 802.1Q 的帧格式

如图 5-25 所示，每一个 802.1Q Tag 中都有一个 Pri 域，该域由三个 bit 为组成，取值范围是 0~7。802.1P 优先级就是根据 Pri 的域值来决定数据帧的优先级。通过交换机的配置页面可配置不同的 Pri 域对应不同的优先级，交换机发送数据帧时，会根据数据帧的 Tag 决定发送的优先级。对于 Un tagged 帧，交换机则按照该入口端口的默认优先级对数据帧进行 QoS 处理。

3. DSCP 优先级

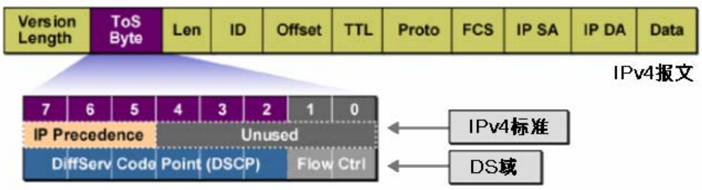


图 5-26 IP 报文

如图 5-26 所示，IP 报文头部的 ToS（Type of Service，服务类型）字段共有 8bit，可以表征不同优先级特征的报文，前 3 个 bit 表示的是 IP 的优先级，取值范围是 0~7。RFC2474 重新定义了 IP 报文头部的 ToS 域，称之为 DS 域。其中 DSCP（Differentiated Services Codepoint，差分服务编码点）优先级用该域的前 6 个 bit（0～5bit）表示，取值范围为 0～63，后 2 个 bit（6、7bit）是保留位。通过交换机的配置页面，可以配置不同的 DS 字段对应不同的优先级，交换机发送 IP 包时，会根据 IP 包的 DS 域决定发送的优先级。对于非 IP 包，交换机则根据是否启用 802.1P 优先级以及数据帧是否带有 Tag 来决定采用哪种优先级模式。

说明：

当启用 802.1P 优先级时，根据数据包是否带有 802.1Q Tag 确定使用哪种优先级模式。对于带有 Tag 的数据包，应用 802.1P 优先级；否则应用 Port 优先级。当启用 DSCP 优先级的时候，如果数据包是 IP 包，则应用 DSCP 优先级；对于非 IP 包，交换机则根据是否启用 802.1P 优先级以及数据帧是否带有 Tag 来决定采用哪种优先级模式。

5.4.2.2 调度模式

在网络拥塞时，通常采用队列调度来解决多个数据流同时竞争使用资源的问题。TL-SG2224P 交换机共实现了 8 个调度队列，TC-0 到 TC-7，其中 TC-0 对应最低优先级的队列，TC7 对应到最高优先级的队列。同时，TL-SG2224P 交换机共提供了四种调度模式，分别是严格优先级模式（SP）、加权轮询优先级模式（WRR）、SP+WRR 模式和无优先级模式（Equ）。

1. SP-Mode：严格优先级模式。SP 队列的调度算法是交换机优先转发当前优先级最高的数据帧，等最高优先级数据帧全部转发完后，再转发次高级优先级的数据帧。TL-SG2224P 交换机有 8 个出口队列，依次为 TC 0-TC 7，在 SP 队列模式下他们的优先级依次升高。SP 队列的缺点是，在拥塞发生时，如果较高优先级队列中长时间有报文存在，那么低优先级队列中的报文就会由于得不到服务而“饿死”。

2. WRR-Mode：WRR 优先级模式。WRR 队列的调度算法是在队列之间按权重比值进行轮流调度，以保证每个队列都得到一定的服务时间。加权值表示获取资源的比重。WRR 队列避免了采用 SP 调度时低优先级中的报文可能长时间得不到服务的缺点，并且虽然多个队列调度是轮询进行的，但是对每个队列不是固定的分配服务时间，如果队列为空则马上更换下一个队列调度，这样可以充分利用带宽资源。默认的权重比是 1:2:4:8:16:32:64:128。

3. SP+WRR-Mode：SP+WRR 优先级模式，这种队列调度模式是前两种模式的混合。在这种模式下，交换机提供了三个调度组，分别是 SP Group，WRR Group0，WRR Group1。其中 SP Group 的成员队列和 WRR Group 之间遵循的是严格优先级调度模式，而 WRR 模式下两个组内部遵循的是 WRR 调度模式。

   如队列 0 和队列 7 是属于 SP Group 的;队列 1，2，3 是属于 WRR Group1，权重比是 1:2:4；队列 4，5，6 是属于 WRR Group0，权重比是 1:2:4；这样在调度时首先是队列 7 按照 SP 的调度模式独自占用带宽，然后是 WRR Group1 组的成员队列 4，5，6 按照权重比 1:2:4 的比例占用带宽，当以上队列都为空的情况下 WRR Group0 的队列 1,2,3 按照权重比 1:2:4 的比例占用带宽，最后是队列 0 独自占用带宽。

4. Equ-Mode：无优先级模式。这种模式下所有队列公平的占用带宽，实际上这是 WRR 模式的一种特殊情况，所有的队列权重比是 1:1:1。

5.4.3 WEB界面配置

点击**服务质量（QoS）**您可以看到：



5.4.3.1 全局配置

本页可以对交换机 QoS 功能进行全局设置。包括以下设置（如下图）：



图 5-27 端口优先级配置

优先级模式： 交换机实现了三种优先级模式，分别是“基于端口的优先级”、“基于 802.1p 的优先级”和“基于 DSCP 的优先级”。其中基于 802.1p 的优先级和基于 DSCP 的优先级模式是可选的，而基于端口的优先级模式默认是启用的。

调度模式： TL-SG2224P 交换机共提供了四种调度模式分别是 SP-Mode，WRR-Mode，SP+WRR-Mode，Equ-Mode。

5.4.3.2 基于端口的优先级

本页面对基于端口的优先级进行配置。包括以下设置（如下图）：



图 5-28 基于端口优先级配置

优先级等级： 有八个选择等级，分别对应到出口队列的 TC 0-TC 7。默认情况下是将所有端口对应到出口队列 TC 0。

说明：

优先等级 TC 0-TC 7，数字越高，表示优先级越高。

5.4.3.3 802.1p优先级

本页面对 IEEE 802.1p 优先级进行配置。包括以下设置（如下图）：



图 5-29 802.1p 优先级

优先级 Tag： 为 IEEE802.1p 协议里规定的 8 个优先级等级。

对应优先级等级： 总共有八个选项，分别对应到出口队列 TC 0，TC 1，TC 2，TC 3，TC 4，TC 5，TC 6，TC 7。在默认情况下是两者的对应关系是 0-TC 2，1-TC 1，2-TC 0，3-TC 3，4-TC 4，5-TC 5，6-TC 6，7-TC 7。

注意：

如无特殊需要，请不要更改优先级 Tag 与优先级等级之间的对应关系。

5.4.3.4 DSCP优先级

本页对 DSCP 的优先级进行配置。主要包括以下设置（如下图）：



图 5-30 DSCP 优先级

对应优先级等级： 总共有八个选项，分别对应到 8 个不同等级的出口队列。在默认情况下前 8 个 DSCP 值对应到优先级级别 0，紧邻的 8 个 DSCP 值对应到优先级级别 1，以此类推。

注意：

如无特殊需要，请不要更改 DSCP 值与优先级等级之间的对应关系。

5.5 802.1X认证

5.5.1 802.1X概述

802.1X 协议是 IEEE802 LAN/WAN 委员会为了解决无线局域网网络安全问题提出的。后来该协议作为局域网端口的一个普通接入控制机制应用于以太网中，主要用于解决以太网内认证和安全方面的问题，在局域网接入设备的端口这一级对所接入的设备进行认证和控制。

TL-SG2224P 交换机可以作为一个认证系统来对您的网络中的计算机进行认证。连接在端口上的用户设备如果能通过交换机认证，就可以访问局域网中的资源；如果不能通过交换机认证，则无法访问局域网中的资源。

5.5.1.1 802.1X概念

支持 802.1X 的系统是采用典型的 Client/Server 体系结构，包括三个实体：

- 客户端：局域网中的一个实体，多为普通计算机，用户通过客户端软件发起 802.1X 认证，并由设备端对其进行认证。客户端软件必须为支持 802.1X 认证的用户终端设备。
- 设备端：通常为支持 802.1X 协议的网络设备，如 TL-SG2224P 交换机，为客户端提供接入局域网的物理/逻辑端口，并对客户端进行认证。
- 认证服务器：为设备端提供认证服务的实体，建议使用 RADIUS 服务器来实现认证服务器的认证和授权功能。该服务器可以存储客户端的相关信息，并实现对客户端的认证和授权。为了保证认证系统的稳定，可以为网络设置一个备份认证服务器。当主认证服务器出现故障时，备份认证服务器可以接替认证服务器的工作，保证认证系统的稳定。

组网图如 图 5-31 所示：

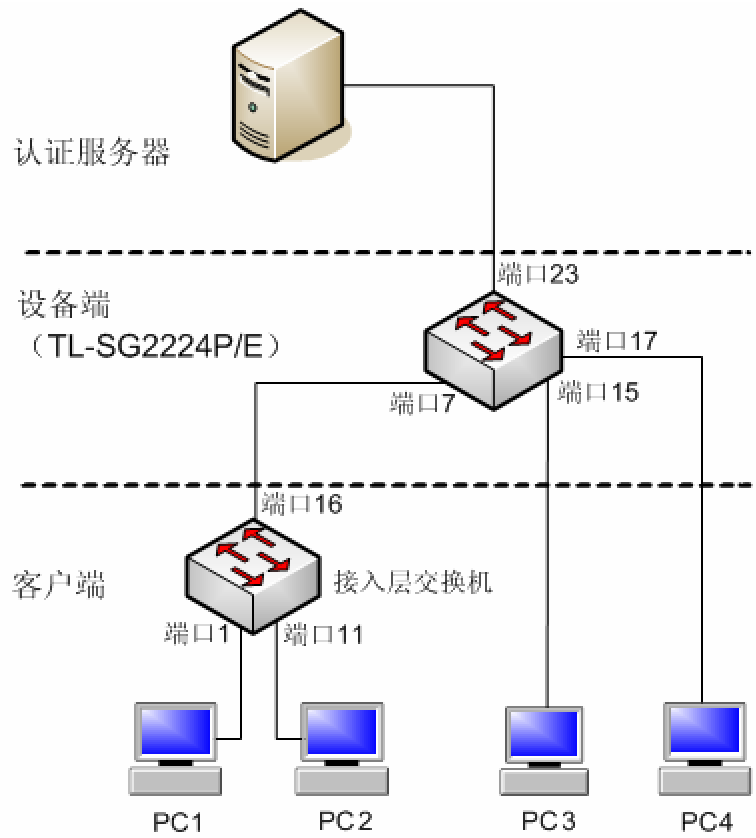


图 5-31 802.1X 系统的典型体系结构

5.5.2 系统配置

通过 WEB 界面对交换机进行配置分为以下几个方面：

1. 在 802.1X 功能系统参数设置中，可以设置该交换机中 802.1X 功能的关闭/启用状态、认证方法（EAP-MD5/PAP）、认证服务器以及计费服务器的 IP 地址等项目。
2. 开启 802.1X 功能时，将同时选择开启的 802.1X 认证是基于端口模式还是基于 MAC 地址模式，在后续的章节将为您介绍两种认证模式的区别。
3. 在端口配置界面，勾选以开启相应物理端口的 802.1X 特性。对于已开启全局 802.1X 功能而没有开启 802.1X 特性的物理端口，这些物理端口下的计算机无须认证也可以访问网络。
4. 在认证过程中，交换机会同时启动多个定时器（例如静默定时器），来控制接入用户与交换机之间进行合理、有序的信息传递，同时也可以进行最大传输次数及响应超时的时间长度等参数的设置。
5. 认证方法（EAP-MD5/PAP）决定了用户端、认证服务器以及交换机之间进行认证信息的交互的过程。

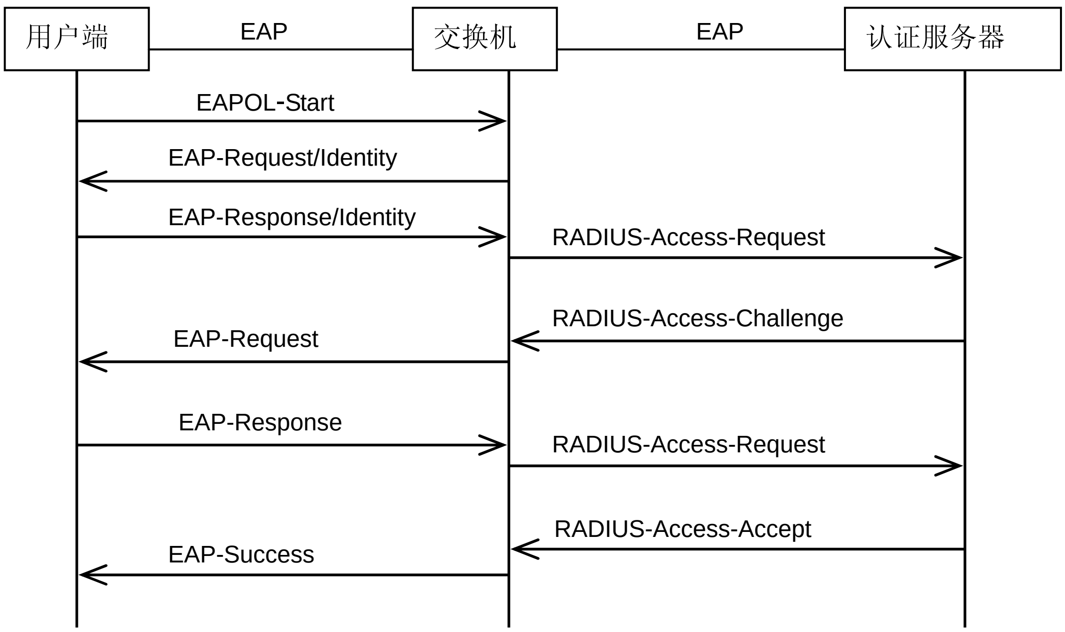


图 5-32 EAP-MD5 认证流程

当交换机工作于 EAP-MD5 模式时，交换机与认证服务器之间也运行 EAP 协议，EAP 帧中封装认证数据，将该协议承载在其它高层次协议中(如 RADIUS)，以便穿越复杂的网络到达认证服务器。

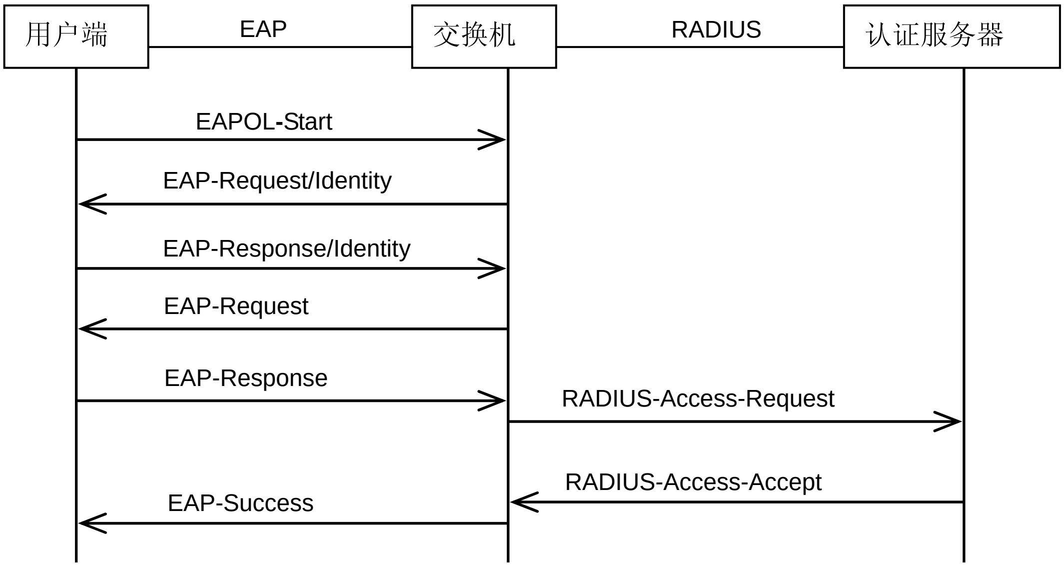


图 5-33 PAP 认证过程

当认证系统工作于 PAP 模式时，仅用户端与交换机之间运行 EAP 协议，交换机终结 EAP 消息，并转换为其它认证协议(如 RADIUS)，传递用户认证信息给认证服务器系统。

注意:

在认证服务器反馈认证通过信息后，交换机会给计费服务器发送计费请求。待计费服务器反馈开始计费信息后交换机才对相应的用户授权。

接下来分别介绍交换机提供的两种认证方法，基于端口的认证和基于 MAC 地址的认证。

5.5.2.1 基于端口的认证

当选择基于端口认证模式时，端口的认证有下面三种状态：

- 自动：该物理端口是需要进行认证的。
- 强制已认证：表示该物理端口不需要认证即可访问网络。
- 强制不认证：表示该物理端口永远无法通过认证，相当于物理断开。

对于某个开启了基于端口认证的物理端口，只要连接到这个端口的第一个用户认证成功后，其他接入用户无须认证就可以访问网络，当第一个用户下线后，其他用户也会被拒绝使用网络。

5.5.2.2 基于MAC地址认证

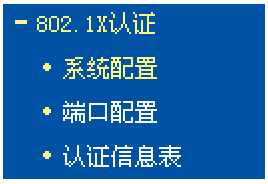
当选择基于 MAC 地址认证模式时，除了强制已认证表和强制不认证表两种特殊的地址外，其他的地址都需要进行认证才能访问网络。

- 强制已认证表列出相应物理端口下不需要向服务器申请认证就已经通过认证并可以访问网络资源的全部主机的 MAC 地址信息。
- 强制不认证表列出了所有物理端口下请求认证却无法通过认证的全部 MAC 地址信息，相应的计算机永远无法通过认证也无法访问网络资源。

基于 MAC 地址认证模式时，相应物理端口下的所有接入用户都要进行单独的认证，当某个用户下线时，也只有该用户无法访问网络而不会影响其他用户。

5.5.3 WEB界面配置

点击 **802.1X** 认证您可以看到：



5.5.3.1 系统配置

本页面对 802.1X 进行系统配置，主要包括以下设置（如下图）：



图 5-34 系统配置

802.1X 状态：	有开启和关闭两种模式。开启模式下，可选择基于端口认证或者基于 MAC 认证。
认证方法：	支持 EAP-MD5 方式和 PAP 方式。
认证服务器 IP：	填写认证服务器的 IP 地址。
认证服务器端口：	认证服务器提供认证服务的逻辑端口，默认为 1812，设置范围 1-65535。
计费服务器 IP：	与认证服务器为同一物理实体，提供计费服务的计算机的 IP 地址。
计费服务器端口：	计费服务器提供计费服务的逻辑端口，默认为 1813，设置范围 1-65535。
服务器密钥：	802.1X 设备端与服务器共享的密钥。
静默、静默时长：	静默为计时器名称，当启用静默计时器时，用户认证失败后，交换机在静默期内不处理此用户的 802.1X 认证请求，设置范围 1-999。
Radius 请求报文最大重传次数：	认证服务器与交换机之间认证报文的最大重复传送次数，设置范围 1-9。

Radius 服务器响应超时时长： Radius 服务器响应的最大等待时间，设置范围 1-9。

客户端请求报文最大重传次数： 交换机和客户端之间认证报文的最大重复传送次数，设置范围 1-9。

客户端响应超时时长： 设备端等待客户端响应的最大等待时间，设置范围 1-9。

5.5.3.2 端口配置



图 5-35 端口配置

勾选相应端口选择开启端口的 802.1X 特性。

注意：

1. 全局 802.1X 特性和端口的 802.1X 特性都开启才能使 802.1X 认证功能生效。
2. 这两个页面的配置数据提交后需要重启交换机才能生效。
3. 认证服务器连接的端口请勿开启 802.1X 特性，且服务器配置参数必须与认证服务器软件的参数一致。

5.5.3.3 基于端口认证

当开启 802.1X认证功能为基于端口认证时，可在 图 5-36、图 5-37 两个界面进行设置及查看：



图 5-36 端口模式配置

自动： 端口需要经过认证服务器认证通过后才能正常使用。

强制已认证： 端口不需要认证服务器认证即能正常访问网络。

强制不认证： 端口永远无法通过认证，相当于物理断开。

注意：

此页面的配置数据提交后需要重启交换机才能生效。



基于端口认证信息表

端口	认证状态	选择	端口	认证状态	选择
1	强制已认证		2	强制不认证	
3	强制不认证		4	未认证	
5	未认证		6	端口802.1X未开启	
7	端口802.1X未开启		8	端口802.1X未开启	
9	端口802.1X未开启		10	强制已认证	
11	端口802.1X未开启		12	端口802.1X未开启	
13	端口802.1X未开启		14	端口802.1X未开启	
15	端口802.1X未开启		16	端口802.1X未开启	
17	端口802.1X未开启		18	端口802.1X未开启	
19	端口802.1X未开启		20	端口802.1X未开启	
21	端口802.1X未开启		22	端口802.1X未开启	
23	端口802.1X未开启		24	端口802.1X未开启	

刷 新 全 选 全不选 选中项重新认证 帮 助

图 5-37 基于端口认证信息表

全选： 选择所有为“已认证”的端口。

全不选： 所有状态为“已认证”的端口均不选。

选中项重新认证： 要求选中的“已认证”端口重新认证。

5.5.3.4 基于MAC地址认证

当开启 802.1X认证功能为基于MAC认证时，可在如 图 5-38、图 5-39、图 5-40 三个界面进行设置及进行查看：



强制已认证表(仅用于基于MAC认证)

端口：1

MAC地址格式：00-0A-EB-00-00-01

序号	MAC地址	状态
1	00-19-66-80-54-36	启用
2	00-19-66-80-52-A5	启用
3	00-19-66-80-53-DE	启用
4	00-19-66-80-54-49	启用
5	00-1D-7D-74-E0-ED	启用
6		启用
7		启用
8		启用
9		启用
10		启用
11		启用
12		启用

提 交 帮 助

图 5-38 强制已认证表



图 5-39 强制不认证表

> **注意:**
> 强制已认证表中的配置数据提交后需要重启交换机才能生效。



图 5-40 认证信息表

MAC 地址： 主机 MAC 地址，格式要求为“XX-XX-XX-XX-XX-XX”，XX 代表十六进制数。

认证状态： 相应 MAC 地址主机的认证状态。

5.5.4 802.1X认证组网应用

5.5.4.1 组网需求

TL-SG2224P 连接一个认证服务器，IP 地址是 192.168.0.20；TL-SG2224P 连接普通计算机以及管理计算机。配置要求如下：

TL-SG2224P 连接管理 PC，MAC 地址为 00-24-32-7A-C0-41，无须认证。

其余计算机均需认证。

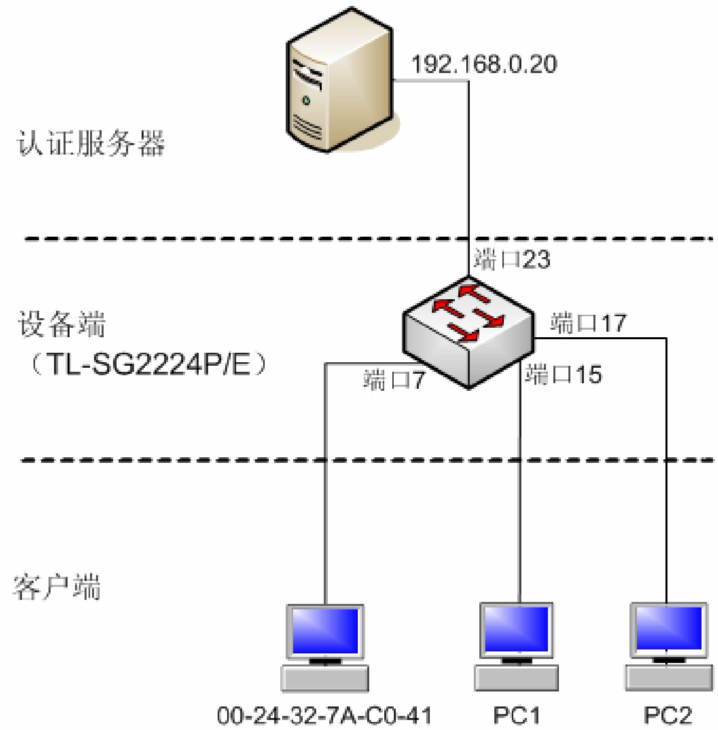
5.5.4.2 组网步骤

首先请确保您的认证服务器已安装了 802.1X 认证的认证软件（如 radius 认证软件）以及在客户端已安装客户端软件（推荐使用我司开发的 TpSupplicant 软件）。TpSupplicant 软件请在光盘中下载安装，具体操作请查阅附录 A。

虽然交换机的认证模式在一个时刻只能基于一种工作模式，但无论是采用基于端口的认证还是基于 MAC 地址的认证，均可以实现上面组网要求。

基于端口认证实现方法：

在基于端口认证模式下，交换机任何开启了 802.1X 认证特性的物理端口都需要进行认证。且一个物理端口下如果通过接入层网络设备接入多台计算机，有一台计算机已经通过认证，那么其他计算机无须认证也可以访问网络。所以若要满足配置要求 2，则此时所有的计算机只能与交换机直接物理连接，如下图所示。

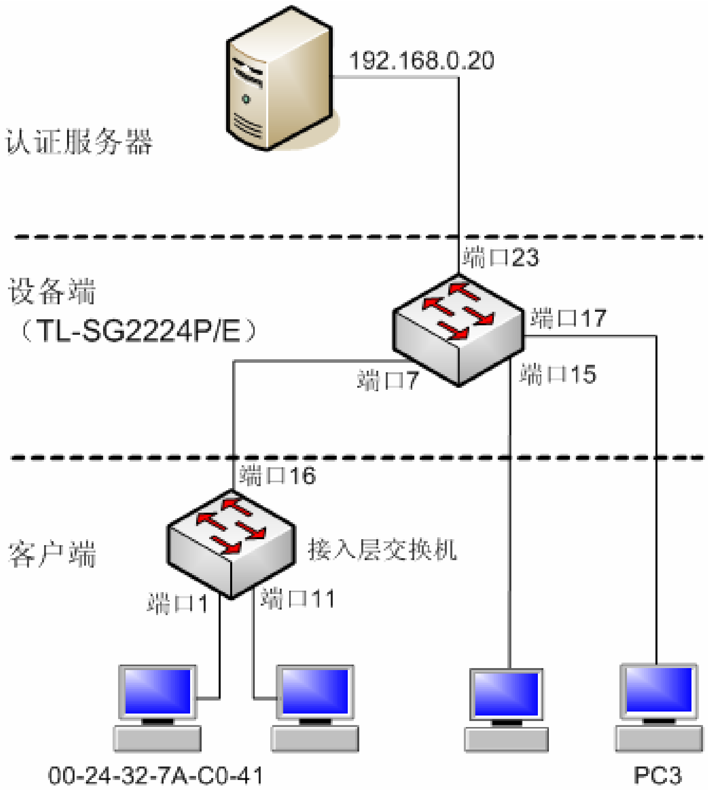


配置步骤如下：

1. 物理连接。管理计算机接交换机端口 7，认证服务器接交换机端口 23。
2. 在系统配置页面开启 802.1X 状态为基于端口认证，同时认证服务器 IP 和计费服务器 IP 均设置为 192.168.0.20。提交配置。
3. 在端口配置页面，勾选开启除端口 7、端口 23 外所有物理端口的 802.1X 特性。提交配置。
4. 在基于端口认证的端口模式配置页面，对所有端口均保持默认的“自动”控制模式。提交配置。
5. 保存并重启交换机。

基于 MAC 认证实现方法：

在基于 MAC 认证模式下，交换机任何开启了 802.1X 认证特性的物理端口下连接的计算机都需要进行认证，同时还可以通过强制已认证表和强制不认证来设置特殊的计算机，例如这里的管理计算机我们可以设置为强制已认证。如下图所示。



配置步骤如下：

1. 物理连接。管理计算机通过接入层交换机接 TL-SG2224P 交换机端口 7，认证服务器接交换机端口 23。
2. 在系统配置页面开启 802.1X 状态为基于 MAC 认证，同时认证服务器 IP 和计费服务器 IP 均设置为 192.168.0.20。提交配置。
3. 在端口配置页面，勾选开启除端口 23 外所有物理端口的 802.1X 特性。提交配置。
4. 在强制已认证表中端口 7 添加管理计算机的 MAC 地址 00-24-32-7A-C0-41 为强制已认证地址。提交配置。
5. 点击保存并重启交换机。

附录A TpSupplicant软件使用说明

安装说明：

1. 查看光盘上面所标的安装路径，然后将安装光盘放入计算机光驱，双击安装软件图标，弹出解压缩对话框，如下图 1 所示。

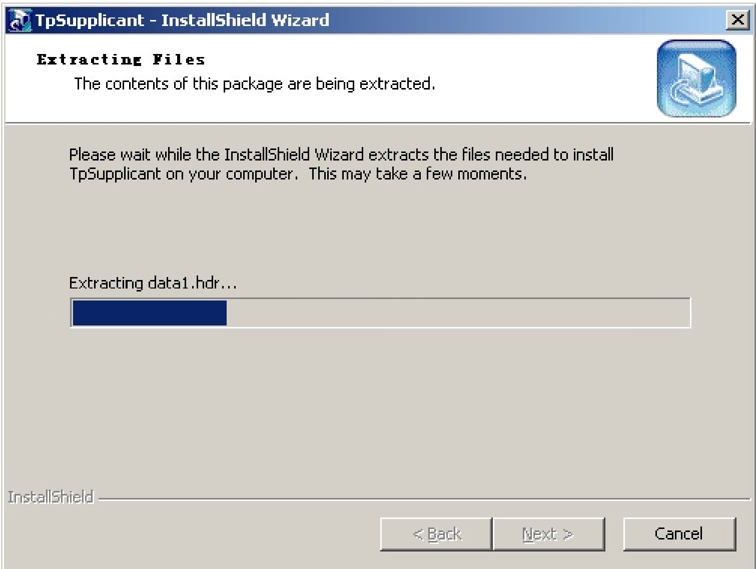


图 1：解压缩对话框

2. 在解压缩过程之后，自动进入安装预备对话框，如下图 2 所示：

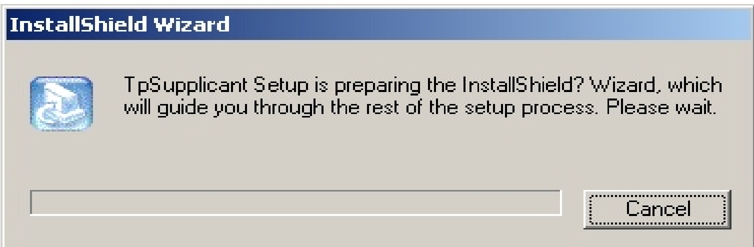


图 2：安装预备对话框

3. 当系统准备工作完成后，欢迎对话框就会显示在屏幕上，此时可点击“Cancel”终止安装过程，如下图 3 所示：

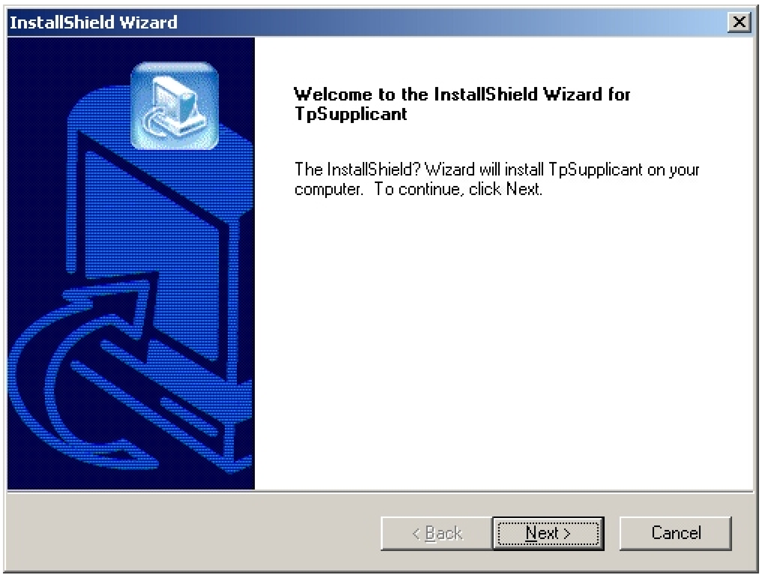


图 3：欢迎对话框

4. 点击“Next”继续安装，下一步显示协议对话框，如下图 4 所示：

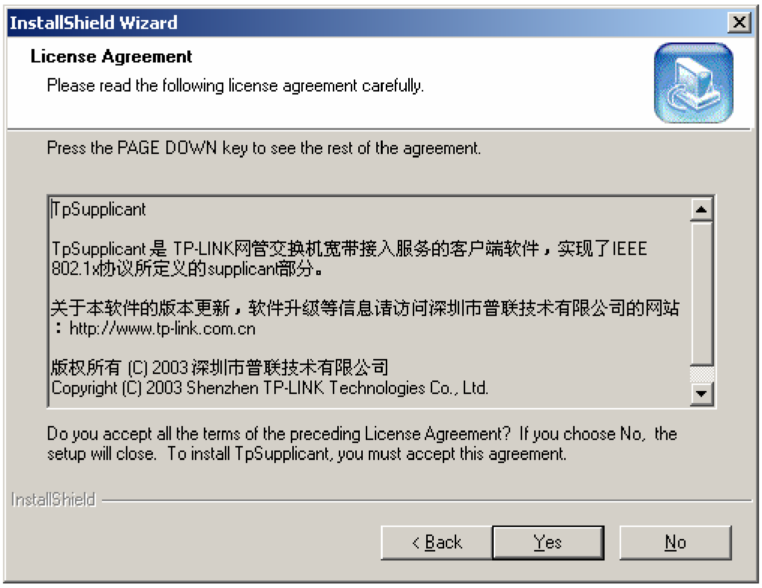


图 4：协议对话框

5. 若不同意该协议，则选择“No”，退出安装。若同意该协议，则选择“Yes”，进行安装路径的选择。如下图 5 所示：

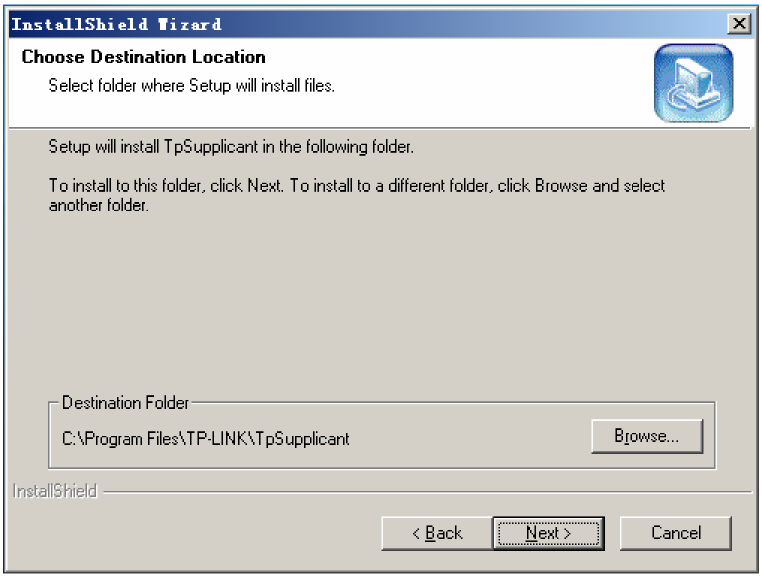


图 5：安装路径对话框

默认路径是系统目录下的 Program Files 目录，点击“Browse”可以选择合适的安装路径。点击“Back”，返回上一个对话框。

6.　点击“Next”进入是选择程序的路径对话框，如下图 6 所示：

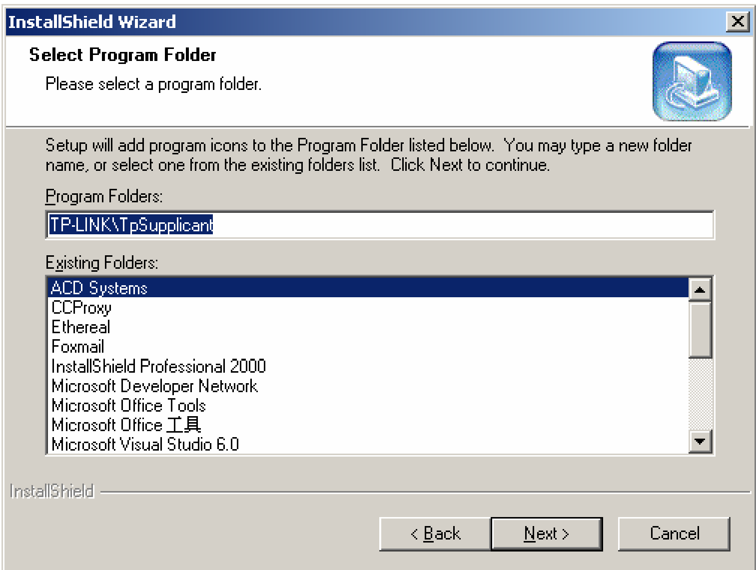
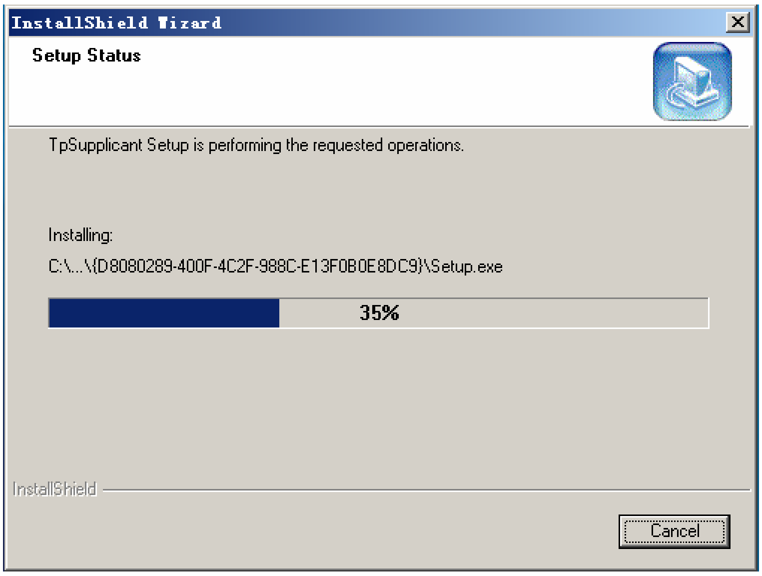


图 6：程序路径对话框

可以修改软件在程序中的路径，但建议保持默认路径。

7.　至此，安装所需参数已确定。点击“Next”，开始安装。



8. 安装完成后，安装完成对话框显示在屏幕上，如下图：

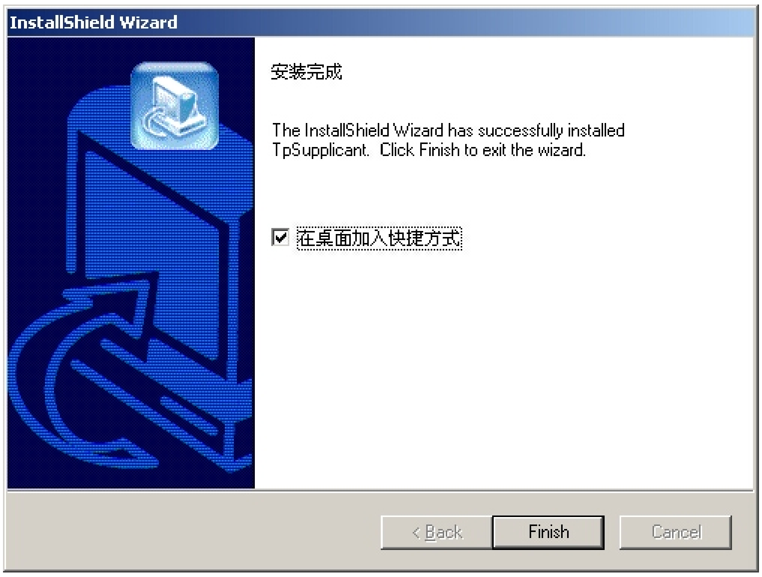


图 7：安装完成对话框

9. 此时可根据需要选择是否在桌面加入快捷方式。如果选择，快捷键就加入到桌面上。通过该快捷键，可快速运行软件。点击“Finish”完成安装。

卸载说明：

当需要卸载 TpSupplicant 软件时，可以按照下面步骤执行：

选择：**开始→程序→TP-LINK→TpSupplicant→Uninstall** 进行 TpSupplicant 软件卸载。软件卸载准备对话框如下图：

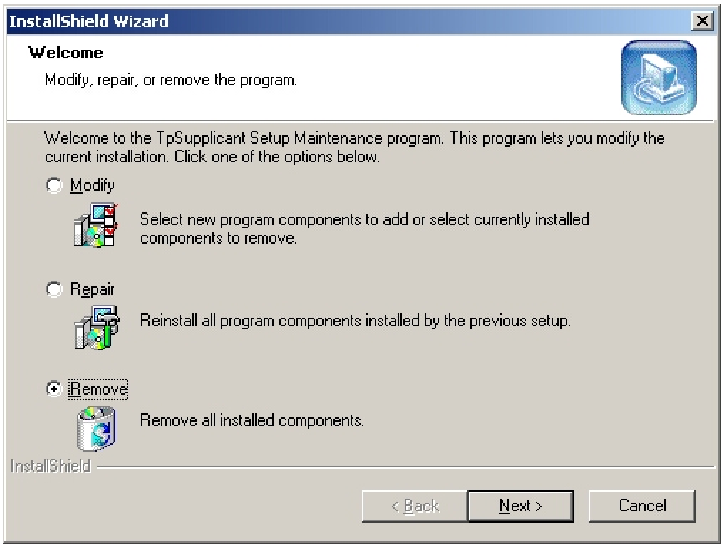
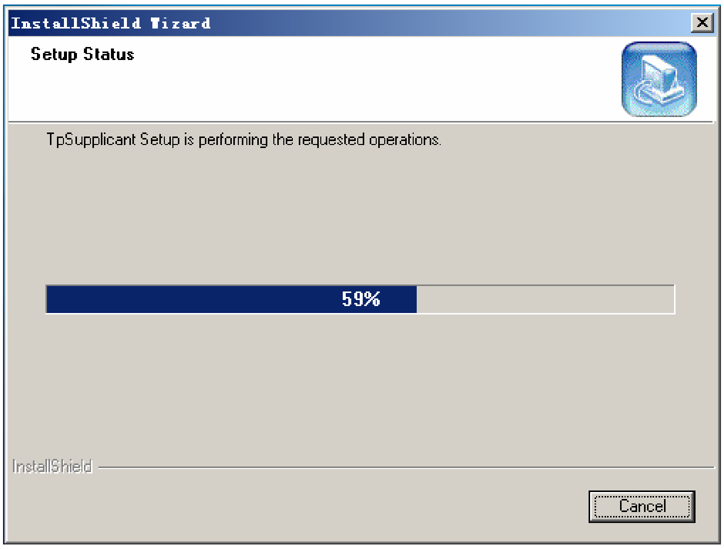
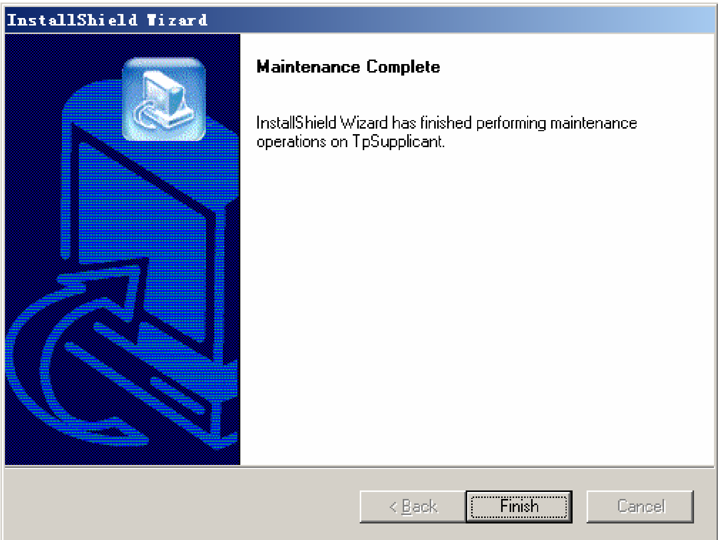


图 8：软件卸载准备

1. 选择“Remove”，并点击“Next”，软件卸载开始进行。



2. 卸载结束后，点击“Finish”关闭窗口即可。



使用说明：

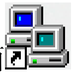
安装完成后，双击桌面图标运行应用程序，弹出程序主对话框如下图所示：



图 9 主对话框

在用户名和密码中输入服务器端设定好的用户名和密码，如果需要自动保存密码请选中保存密码，注意用户名和密码不得多于 15 个字符。

当点击“连接”键时，进行连接；点击“退出”键时，退出应用程序；当点击“属性”键时，弹出属性对话框，可以对拨号属性进行适当的设置，如下图：

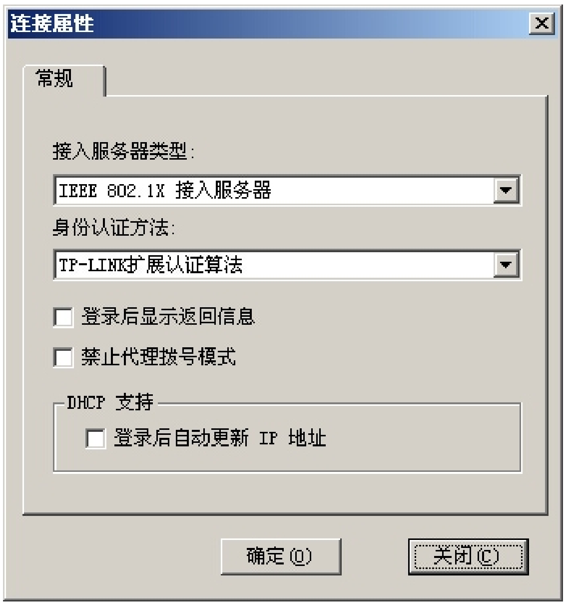


图 10：属性对话框 1

接入服务器类型只可以选择 IEEE 802.1X 接入服务器，身份认证方法有如图示两种：

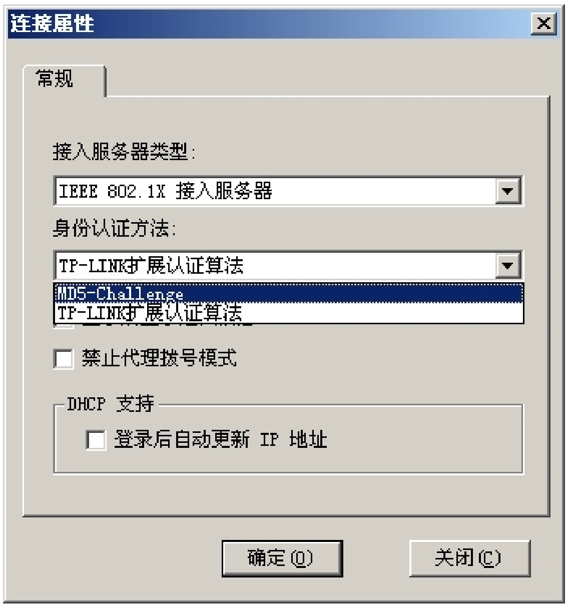


图 11：属性对话框 2

MD5-Challenge 是使用 EAP（扩展认证协议）认证的时候要选择的，此时交换机要在 IEEE802.1X 的认证属性的认证方法上选择“EAP Authentication”认证。

TP—LINK 扩展认证算法是使用用户名密码方法认证的时候要选择的，此时交换机要在 IEEE802.1X 的认证属性的认证方法上选择“PAP Authentication”认证。

如果选中**登陆后显示返回信息**，当交换机将 Radius 返回的信息返回给客户端时该软件可以将返回信息显示给用户，如果不选择则不会显示这样的信息。

如果选中**登陆后自动更新 IP 地址**，此时网络需要一个 DHCP 服务器来为客户端分配 IP 地址；如果没有选择则需要用户自己设置 IP 地址。

注意：

此处请勿选择**禁止代理拨号模式**。

在主窗口下如果点击连接，则显示如下认证状态对话框：



图 12：认证状态对话框

此时表示的状态是正在查找认证服务器。

当顺利的通过认证后，会显示一个认证通过对话框，如下图所示：



图 13：认证通过对话框

图中对话框中显示的账号剩余时间是当 Radius 服务器返回这样的信息并且选中登陆时显示返回信息的时候才会出现的。

该对话框持续一小段时间后就会消失，此时在系统任务栏下有一个图标，当用户右击时会出现一个弹出式菜单，选择其中的“显示连接状态”或者双击该图标会显示连接状态对话框，如下图所示：



图 14：连接状态对话框

如果选择菜单下的关于时，会显示关于该软件的信息，如下图所示：

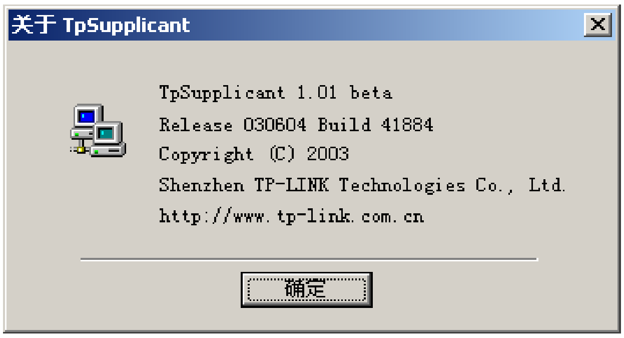


图 15：关于对话框

常见问题：

1. 当我运行该软件的时候为什么会出现如下图所示的错误对话框？



图 16：缺失 DLL 对话框

答：如果出现图 16 对话框，说明缺少了支持的 DLL 文件，如果安装了该软件请将该软件卸载掉后重新安装，如果没有安装的话只需要重新安装，然后重新运行。

2. 当我的系统使用了多于一个 IP，会有什么现象？



图 17：增加 IP 地址后的错误对话框

答：如果初次启动，经过 20 秒会断连；如果在启动的时候动态修改 IP，5 秒钟会断连。紧接着出现图 17 对话框，整个应用程序退出。

3. 可以使用该软件拨号其他公司生产的交换机吗？

答：不可以，该软件是专门为我司交换机定制。

4. 当我运行该软件的时候为什么显示找不到网卡，可我的网卡运行良好？如下图的对话框：



图 18：找不到网卡对话框

答：系统中缺失了驱动，如果安装了该软件请卸载该软件，然后重新安装，如果没有安装请重新安装，然后再运行。

5. 如果我设置保存密码会不会不安全？

答：不会，密码被保存到注册表中并且已经经过加密。

附录B 常见故障处理

问题 1：为什么我买的交换机没有 UPLINK 口？

答：UPLINK 端口出现在一些旧式的交换机产品上，它为方便交换机与交换机级联时的网线选择而设计。目前我司生产的交换机均支持端口自动翻转（Auto MDI/MDIX）功能，没有专门的 UPLINK 端口，任一端口都可以作为级联口使用。

问题 2：交换机启动后所有指示灯全都亮（即便是没有插网线的端口），怎么办？

答：交换机启动后所有指示灯全亮（即便是没有插网线的端口），通常由交换机的电源模块出现故障导致，请返厂维修。返修的途径可通过经销商或我司离其较近的办事处。

问题 3：交换机出现部分端口不通的问题该如何处理？

答：当交换机上出现部分端口不通时，可能是网线故障、网卡故障和交换机端口故障，可通过如下测试定位故障：

- 连接的计算机和交换机端口保持不变，更换其它网线；
- 连接的网线和交换机端口保持不变，更换其它计算机；
- 连接的网线和计算机保持不变，更换其它交换机端口；
- 若确认为交换机端口故障，请联系返厂维修。

问题 4：端口自适应状态检测的顺序如何？

答：端口对状态进行检测时是按如下顺序进行：1000M 全双工，100M 全双工，100M 半双工，10M 全双工，10M 半双工，从高到低依次检测，并自动以所支持的最高速度连接。

问题 5：Trunk 功能适合哪些具体应用？

答：Trunk 功能比较适合于以下方面具体应用：

- Trunk 功能用于交换机与服务器之间的相联，为服务器提供独享的高带宽；
- Trunk 功能用于交换机之间的级联，为交换机之间的数据交换提供高带宽的数据传输能力，提高网络速度，突破网络瓶颈，进而大幅提高网络性能。

问题 6：如何设置端口监控功能?

答：端口监控包括“监控模式”、“监控端口”和“被监控端口”的设置。“监控模式”一般选择“输入输出监控”；连接监控主机对应的交换机端口设置成“监控端口”，连接外部宽带网络对应的交换机端口设置成“被监控端口”。一般情况下，“被监控端口”建议只设置一个。

问题 7：端口安全、动态地址表、静态地址表具体实现的是什么样的功能？

答：通常将静态地址表与端口安全结合，应用在“网络管理员希望将交换机每端口的主机都固定，不允许随便拔网线换端口”等场合。

- 端口安全：某个端口的端口安全启动时，该端口将不再学习新的 MAC 地址，同时只发送符合条件的数据帧，其他的帧将被丢弃。判断条件为：发往交换机的帧，如果其源地址为该端口的 MAC 地址表成员，则允许转发，否则将被丢弃。例如：原先 A 电脑接交换机的 1 端口并且将 A 电脑的 MAC 地址与端口 1 加到静态地址表，接着 1 端口开启了端口安全功能，此时若有一台 B 电脑替换 A 电脑接在 1 端口，那么 B 电脑就不能使用网络资源。

- 静态地址表：静态地址表记录了端口的静态地址，表中一个 MAC 地址对应一个端口（一个端口可对应多个 MAC 地址），设置后所有发给这个地址的数据将只会转发到该端口。
- 动态地址表：动态地址表包含两项内容，MAC 地址及其对应的端口号。动态地址表是动态更新的，表里的每一个记录都是有寿命限制的，其寿命长短受最大老化时间控制。
- 无论是动态地址表还是静态地址表，~~他~~它们共同的基本作用是给需要转发的数据帧指明目的端口。

问题 8：VLAN 功能有哪些应用？

答：VLAN（Virtual Local Area Network）即虚拟局域网，是一种通过将局域网的设备逻辑上而不是物理的划分成一个个局域网从而实现虚拟工作组的技术。VLAN 具有增强网络安全和提升网络性能的优点。一般应用在企业网络中，如实现研发、财务、销售各个部门之间不能互相访问，保障企业信息安全。

附录C 出厂设置

主功能项	功能子项	WEB 页面细则		出厂设置值
系统管理	系统标识	系统名称		空
		系统位置		空
		联系方法		空
	网络参数	DHCP Client		禁用
		IP 地址		192.168.0.1
		子网掩码		255.255.255.0
		默认网关		空
	用户安全	管理员用户	用户名	supervisor
			口令	supervisor
		普通用户	状态	未启用
			用户名	guest
			口令	guest
		安全配置	身份过滤	禁用
			管理人数限制	禁用
	时间设置	手动设置	状态	启用
			日期	2006 年 1 月 1 日
			时间	08 时 00 分 00 秒
		NTP	状态	未启用
			首选 NTP 服务器	133.100.9.2
			备选 NTP 服务器	139.78.100.163
			时区	（GMT+08:00）北京
		获取管理 PC 时间		未启用
	软件升级	升级系统文件		空
	系统备份	配置文件备份与载入		空
端口管理	基本参数	端口状态		启用
		端口安全		禁用
		流量控制		禁用
		协商方式		自协商
	端口汇聚	Trunk 组号		1
		选路算法		MAC、IP 及传输层端口
		Trunk 组成员		空
		广播抑制		禁用

主功能项	功能子项	WEB 页面细则	出厂设置值
		多播抑制	禁用
		UL 包抑制	禁用
	端口镜像	监控模式	禁用
		监控端口	1
	端口限速	入口带宽限制	禁用
		出口带宽限制	禁用
	风暴抑制	多播抑制	禁用
		广播抑制	禁用
		UL 包抑制	禁用
	流量统计	端口	1
	端口描述	端口描述	空
地址表管理	静态 MAC 绑定	对应端口	1
	MAC 过滤	MAC 过滤	空
	地址老化时间	MAC 地址最大老化时间	300 秒
	动态 MAC 绑定设置	地址绑定	禁用
	动态 MAC 绑定	动态 MAC 绑定	空
VLAN 管理	VLAN 模式配置	VLAN 模式配置	不设置 VLAN
	Port VLAN 配置	Port VLAN 配置	所有端口均属于 VLAN 1
	Tag VLAN 全局配置	缺省 VID	1
		Un tag 帧处理	通过
	Tag VLAN 配置	Tag VLAN 配置	所有端口属于 VLAN 1，VID 为 1，出口规则为“去 Tag”
	MTU VLAN 配置	上联端口	1
ARP 攻击防护	全局配置	ARP 攻击防护功能	禁用
		特殊端口配置	空
	主机绑定	主机绑定	空
	非法 ARP 统计	非法 ARP 统计	空
网络优化	IGMP 配置	IGMP 侦听	禁用
	组播成员列表	组播成员列表	空
服务质量（QoS）	全局配置	基于端口	启用
		基于 802.1p	未启用
		基于 DSCP	未启用
		调度模式	Equ-Mode

主功能项	功能子项	WEB 页面细则	出厂设置值
	端口优先级	优先级等级	TC 0
	802.1P 优先级	802.1P 优先级	0-TC 2，1-TC 1，2-TC 0，3-TC 3，4-TC 4，5-TC 5，6-TC 6，7-TC 7
	DSCP 优先级	DSCP 优先级	0~7-TC 0，8~15-TC 1，16~23-TC2，24~31-TC3，32~39-TC4，40~47-TC5，48~55-TC 6，56~63-TC 7
802.1X 认证	系统配置	802.1X 状态	全局关闭 802.1X
		认证方法	EAP-MD5
		静默	关闭
		静默时长	10 秒
		Radius 请求报文最大传送次数	3
		Radius 服务器响应超时时长	3 秒
		客户端请求报文最大传送次数	3
		客户端响应超时时长	3 秒
	端口配置	端口配置	空
	认证信息表	基于端口认证信息表	空
系统工具	重启与复位	重启和复位	空
	Ping 检测	目标 IP 地址	192.168.0.1
		发送次数	4
		发送报文长度	64 字节
		时间间隔	1000 毫秒
	线缆检测	检测端口	--
	系统日志	系统日志	空

附录D 术语表

	英文术语	中文名称	定义或描述
A	ACL(Access Control List)	访问控制列表	访问控制列表可用来授权、拒绝、限制访问设备、特性或应用。
	ARP (Address Resolution Protocol)	地址解析协议	一种把 IP 地址转换成物理地址的协议。
	Auto-Negotiation	自协商	使交换机等设备两端按照最大的性能来自动协商工作速率和双工模式。
B	Broadcast Storm	广播风暴	通过一个单端口在网络上同时发送过量广播帧。转发信息的响应在网络中将会堆积起来，消耗过多的网络资源或造成网络超时。
	Broadcasting	广播	向网络中的所有网点发送数据的转发形式。
	Broadcast Domain	广播域	可接收指定集合内任意设备发出的广播帧的设备集合。路由器能够限制广播域，是因为路由器不转发广播包。
C	Combo Port	Combo 端口	同一个逻辑端口具有两个物理连接，包括一个 RJ-45 连接和一个 SFP 连接，对于 RJ45 和 SFP 两种连接，同一时间只有一种可以生效。
	CoS（Class of Service）	服务等级	即 802.1p 优先级方案。CoS 提供了为数据包加入优先级标签的方法，将报文分为 8 个级别。值的范围：0～7。
D	DHCP（Dynamic Host Configuration Protocol）	动态主机配置协议	为网络中的主机动态分配 IP 地址、子网掩码、网关等信息。
	DHCP Client	DHCP 客户端	网络上使用 DHCP 获得网络地址等配置参数的主机。
	DSCP（DiffServe Code Point）	差分服务编码点	封装在 IP 报文头的一个 6 位域中，可以将报文分为 64 个级别。取值范围：0～63。
E	EAP（PPP Extensible Authentication Protocol）	PPP 的扩展认证协议	用于 PPP 认证，可以支持多种认证机制
	Ethernet	以太网	以太网使用总线形或星形拓扑且支持的传输速率达到 10Mbps 数量级。称为快速以太网的新版本速率可达 100Mbps。以太网遵行 IEEE 802.3 标准。以太网是最普遍使用的局域网标准。
F	Flow Control	流控	流控使低速设备能够和高速设备通讯。这种流控是通过高速端口暂停发包的方式，以达到高速端口发包速度与低速端口收包速度匹配。
	Frame	帧	含有物理介质层所需的头和尾信息的数据包。
	Full-Duplex	全双工	采用 IEEE802.3x 标准，在一个时刻能可同时进行接收和发送两个方向的数据操作。

	英文术语	中文名称	定义或描述
G	GBIC（Giga Bitrate Interface Converter）	千兆接口转换器	网络设备连接到光纤传输系统的硬件模块，进行光电转换。
H	Half-Duplex	半双工	采用 Backpressure 标准，在一个时刻只能进行收或发一个方向的数据操作。
I	IGMP（Internet Group Management Protocol）	互联网组管理协议	规定了主机与三层组播设备之间建立和维护组播组成员关系的机制。
	IEEE 802.1p		在数据链路层的介质访问控制子层上对网络流量加入优先级。
	IEEE 802.1q		定义 VLAN 桥的操作。在桥式局域网结构中允许对 VLAN 的管理、定义和操作。
	IEEE 802.1X	基于端口的访问控制	为受保护网络提供认证、控制用户通信以及动态密钥分配等服务的有效机制。
L	LAN（Local Area Network）	局域网	指将位于相对有限区域内的一组计算机、打印机和其他设备连接起来的通讯网络。LAN 内部连接的设备都能与其中的其他设备交互。
M	MAC(Media Access Control)	介质访问控制协议	MAC 协议主要负责控制与连接物理层的物理介质，协议中定义的 MAC 地址是用来标识网络节点的硬件地址。
	Multicast	组播	一种向指定的多个目的地址转发数据的转发机制。
N	NTP Server	网络时间服务器	用于互联网上的计算机时间同步。
P	PAP（Password Authentication Protocol）	密码认证协议	通过 2 次握手提供一种对等结点建立认证的链路控制协议。
Q	QoS（Quality of Service）	服务质量	用来解决网络延迟和阻塞等问题的一种技术。
R	RADIUS(Remote Authentication Dial In User Service)	宽带窄带认证系统服务	通用的认证计费协议，可以采用多种方式登录认证。
S	SFP（Small Form-factor Pluggables）	小型化 GBIC	SFP 模块在功能上与 GBIC 基本一致，体积比 GBIC 模块减少一半。
	Switch	交换机	用来实现交换式网络的设备。在 ISO 的 OSI 模型中，它位于数据链路层，能对以太网帧进行转发操作，可以进行 MAC 地址学习。
T	TCP/IP（Transmission Control Protocol/ Internet Protocol）	传输控制协议和互连网协议	IP 提供无连接的数据报传输机制。TCP 提供一种面向连接的、可靠的字节流服务。

	英文术语	中文名称	定义或描述
	Trunking	端口汇聚	将一组端口捆绑在一起形成一个聚合组，从而达到增加带宽，提高连接可靠性的目的。
	ToS（Type of Service）	服务类型	封装在 IP 报文头的一个 8 位域中，表征不同优先级特征的报文。
U	UDP（User Datagram Protocol）	用户数据报协议	面向无连接的、不可靠的传输层协议。
	UTP(Unshielded Twisted Pair)	非屏蔽双绞线	双绞线外部没有屏蔽介质。
	Unicast	单播	一种向单个目的地址转发数据的转发机制。
V	VLAN (Virtual Local Area Network)	虚拟局域网	组成局域网的逻辑子组。VLAN 是由软件而非硬件实现的。
W	WAN（Wide Area Network）	广域网	在很宽的地理区域内为用户服务的数据通信网络，此网络通常使用由公共设备商提供的传输设备。帧中继和 X.25 都是广域网的例子。

附录E 技术参数规格

参数项	参数内容
支持的标准和协议	IEEE 802.3 10BASE-T 以太网 IEEE 802.3u 100BASE-TX 快速以太网 IEEE 802.3ab 1000BASE-T 千兆以太网 IEEE 802.3z 千兆以太网(光纤) ANSI/IEEE 802.3 NWay 自动协商 IEEE 802.3x 流量控制 IEEE 802.1p 优先级 IEEE 802.1q VLAN 桥操作 IEEE 802.1X 基于端口的访问认证 CSMA/CD Ethernet
数据传输速率	以太网 10Mbps 半双工，20Mbps 全双工 快速以太网 100Mbps 半双工，200Mbps 全双工 千兆以太网 2000Mbps 全双工
网络介质	10BASE-T：2 对 3 类或 3 类以上非屏蔽双绞线(UTP)(≤100m) EIA/TIA-568 100 欧屏蔽双绞线(STP) (≤100m) 100BASE-TX：2 对或 4 对 5 类非屏蔽双绞线(UTP)(≤100m) EIA/TIA-568 100 欧屏蔽双绞线(STP)(≤100m) 1000Base-T：4 对 5 类(推荐超 5 类)非屏蔽双绞线(UTP)(≤100m)
指示灯	电源指示灯、1000Mbps 速率指示灯、Link/Act 指示灯、系统指示灯、风扇指示灯
传输方式	存储转发
背板带宽	48Gbps
MAC 地址学习	自动更新，支持 8K 地址空间
包转发速率	10BASE-T：14881pps/端口 100BASE-TX：148810pps/端口 1000Base-T：1488095pps/端口
交流输入	100-240V~ 50/60Hz
工作温度	0℃~40℃
存储温度	-40℃~70℃
湿度	5%~90%（RH 无凝结）
尺寸（长×宽×高）	440mm×180mm×44mm